



Good Passwords, Bad Passwords, and How to See the Difference

David Klaftenegger

Department of Information Technology
Uppsala University, Sweden

20. January 2020



Caveat Auditor

Background

Passwords

Diceware

Questions

Overture

- this talk contains opinions
- my opinions
- not the university's
- nor do I claim to be an expert
- ... so expect some imprecision and errors



What's the problem?

Why use passwords?

Background

Passwords

Diceware

Questions

Overture



What's the problem?

Why use passwords?

- protect accounts



What's the problem?

Why use passwords?

- protect accounts (so that I can't use them)



What's the problem?

Why use passwords?

- protect accounts (so that I can't use them)
- protect against
 - your ex?
 - your coworkers?
 - police?
 - nation state attackers?



What's the problem?

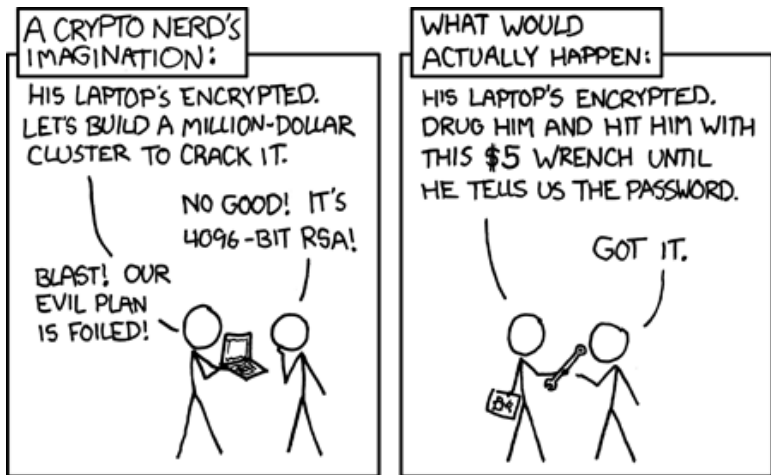
Background

Passwords

Diceware

Questions

Overture



<https://www.xkcd.com/538/>

<https://creativecommons.org/licenses/by-nc/2.5/>



What's the problem?

Why use passwords?

- protect accounts (so that I can't use them)
- protect against
 - your ex?
 - your coworkers?
 - police?
 - nation state attackers?

This talk

- people who know you well
- computers guessing very quickly
- not: people willing to hurt you
- not: attackers with other access



Bad Passwords

Background

Passwords

Diceware

Questions

Overture

Only I myself know how the password is chosen!



Bad Passwords

Background

Passwords

Diceware

Questions

Overture

Only I myself know how the password is chosen!

- The town I live in
- My birthplace, a special character, and two numerals
- "onetwothreefourfivesixseveneight"
- "41229411121620514577518"



Bad Passwords

Background

Passwords

Diceware

Questions

Overture

Only I myself know how the password is chosen!

- The town I live in
- My birthplace, a special character, and two numerals
- "onetwothreefourfivesixseveneight"
- "41229411121620514577518"

Security by obscurity



Bad Passwords

Only I myself know how the password is chosen!

- The town I live in
- My birthplace, a special character, and two numerals
- "onetwothreefourfivesixseveneight"
- "41229411121620514577518"

Security by obscurity

- When someone knows how you construct your password it is trivial to guess it
- Therefore the password should be chosen **randomly**



Choosing Passwords

Background

Passwords

Diceware

Questions

Overture

How to choose good passwords?

- (audience suggestions)



Choosing Passwords

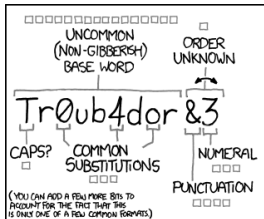
Background

Passwords

Diceware

Questions

Overture



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

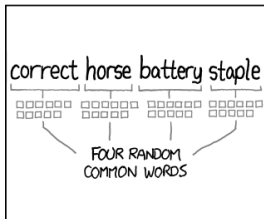
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE: YES, CRACKING A STOKEN MESH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

<https://www.xkcd.com/936/>

<https://creativecommons.org/licenses/by-nc/2.5/>



Good Passwords

Background

Passwords

Diceware

Questions

Overture

Gold Standard

- I tell you **exactly** how I choose my password
- You still cannot guess it before we're all dead



Good Passwords

Background

Passwords

Diceware

Questions

Overture

Gold Standard

- I tell you **exactly** how I choose my password
- You still cannot guess it before we're all dead

Entropy means using randomness

- have a random number generator



Good Passwords

Background

Passwords

Diceware

Questions

Overture

Gold Standard

- I tell you **exactly** how I choose my password
- You still cannot guess it before we're all dead

Entropy means using randomness

- have a random number generator
- use it until you have a secure password



Good Passwords

Background

Passwords

Diceware

Questions

Overture

Please bear with me it's just an example

■ 1



Good Passwords

Background

Passwords

Diceware

Questions

Overture

Please bear with me it's just an example

■ 15



Good Passwords

Background

Passwords

Diceware

Questions

Overture

Please bear with me it's just an example

■ 151



Good Passwords

Background

Passwords

Diceware

Questions

Overture

Please bear with me it's just an example

■ 1512



Good Passwords

Background

Passwords

Diceware

Questions

Overture

Please bear with me it's just an example

■ 15124



Good Passwords

Background

Passwords

Diceware

Questions

Overture

Please bear with me it's just an example

■ 151245



Good Passwords

Background

Passwords

Diceware

Questions

Overture

Please bear with me it's just an example

■ 1512452



Good Passwords

Background

Passwords

Diceware

Questions

Overture

Please bear with me it's just an example

■ 15124524



Good Passwords

Background

Passwords

Diceware

Questions

Overture

Please bear with me it's just an example

■ 151245241



Good Passwords

Background

Passwords

Diceware

Questions

Overture

Please bear with me it's just an example

■ 1512452415



Good Passwords

Background

Passwords

Diceware

Questions

Overture

Please bear with me it's just an example

■ 1512452415263112214316331622221641



Remembering Passwords

Background

Passwords

Diceware

Questions

Overture

Now we have a good password

- can't remember that many numbers in order
- slow to type



Remembering Passwords

Background

Passwords

Diceware

Questions

Overture

Now we have a good password

- can't remember that many numbers in order
- slow to type

Diceware

- transform numbers into words
- much easier to remember
- still equally hard to guess



Diceware

Process

- roll die five times
- write down results (in order)
- look up word in wordlist
- repeat until desired number of words



Diceware

Process

- roll die five times
- write down results (in order)
- look up word in wordlist
- repeat until desired number of words

Example

- 15124 52415



Diceware

Process

- roll die five times
- write down results (in order)
- look up word in wordlist
- repeat until desired number of words

Example

- 15124 52415
- carrot rotunda



Diceware

Process

- roll die five times
- write down results (in order)
- look up word in wordlist
- repeat until desired number of words

Example

- 15124 52415
- carrot rotunda
- 21146 11646 13351 56154



Diceware

Process

- roll die five times
- write down results (in order)
- look up word in wordlist
- repeat until desired number of words

Example

- 15124 52415
- carrot rotunda
- 21146 11646 13351 56154
- correct animal battery staple



Diceware

Process

- roll die five times
- write down results (in order)
- look up word in wordlist
- repeat until desired number of words

Example

- 15124 52415
- carrot rotunda
- 21146 11646 13351 56154
- correct animal battery staple
- 11512 45241 52631 12214 31633 16222 21641



Diceware

Process

- roll die five times
- write down results (in order)
- look up word in wordlist
- repeat until desired number of words

Example

- 15124 52415
- carrot rotunda
- 21146 11646 13351 56154
- correct animal battery staple
- 11512 45241 52631 12214 31633 16222 21641
- ambiguity premium sampling apostle gallstone clumsily
CURSOR



Diceware

How secure is it?

Background

Passwords

Diceware

Questions

Overture



Diceware

Background

Passwords

Diceware

Questions

Overture

How secure is it?(roughly)

dice rolls	10 numerals	26 letters	52 case-sensitive	88 with symbols	diceware
5	4	3	2	2	1 word
10	8	5	5	4	2 words
15	12	8	7	6	3 words
20	16	11	9	8	4 words
25	19	14	11	10	5 words
30	23	16	14	12	6 words
35	27	19	16	14	7 words
40	31	22	18	16	8 words



Diceware

Background

Passwords

Diceware

Questions

Overture

<https://www.eff.org/dice>

https://www.eff.org/files/2016/07/18/eff_large_wordlist.txt

https://en.wikipedia.org/wiki/Password_strength

<https://haveibeenpwned.com/>



Questions?

Background

Passwords

Questions

Overture



<https://www.xkcd.com/1256/>

<https://creativecommons.org/licenses/by-nc/2.5/>



Use Different Passwords

Background

Passwords

Diceware

Questions

Overture

Remember all these passwords?

- **always** use a different password
- you only need one memorable password
- store the others in a password manager