

Password strength meters

Schwarenthorer Yannick

Just colored words

Facebook

New:

Too short

Re-type new:

Passwords match

Baidu

Password:

Confirm Password:

The structure of your password is too simple to replace the more complex the password, otherwise unable to register successfully. Password length of 6 to 14, the letters are case-sensitive. [Password is too simple hazards](#)

Green bars / Checkmark-x

Twitter

✖ Password is too obvious.

✔ Password is okay.

✔ Password is perfect!

Checklists

Apple

Password strength: weak

Password must:

- Have at least one letter
- Have at least one capital letter
- Have at least one number
- Not contain more than 3 consecutive identical characters
- Not be the same as the account name
- Be at least 8 characters

Segmented bars

Weibo

* Create a

Уровень сложности: слабый

Уровень сложности: сильный

Mail.ru

Уровень сложности: слабый

Уровень сложности: сильный

Paypal

Fair

- ✔ Include at least 8 characters
- ✔ Don't use your name or email address
- Use a mix of uppercase and lowercase letters, numbers, and symbols
- ✔ Make your password hard to guess - even for a close friend

Strong
 Fair
 Weak

Yahoo.jp and Yahoo

baseball1 低 Strong

Aaaaaa1! 中 Very strong

Gradient bars

Wordpress.com

Bad

Live.com

Weak

Medium

Strong

Color changing bars

Mediafire

Password Strength Too short

Password Strength Weak

Password Strength Fair

Password Strength Good

Password Strength Strong

Blogger

Password strength: Weak

Google

Create a password

Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. [Why?](#)

Password strength: Strong

Password strength: Good

Password strength: Too short

Password meters

- No documentation of design choices etc. (expect for Dropbox)
- Mostly only counting of character classes (LUDS)
- Inconsistent and badly implemented

ZID password guidelines

- Das Passwort sollte mindestens 8 Zeichen lang sein und aus einer Mischung von Buchstaben, Ziffern und Satz- oder Sonderzeichen bestehen.
- Verwenden Sie **keinesfalls** Ihren Benutzernamen oder anderen Namen (wie z.B. Vor- oder Nachname) oder Informationen, die in unmittelbarem Zusammenhang mit Ihnen stehen, wie Geburtstag, Telefonnummer, Sozialversicherungsnummer, Ausweisnummer, Autonummer, Hausnummer, Wohnort, Straße usw.
- Benutzen Sie keine Buchstabenfolgen von der Tastatur wie "qwertz" oder ähnliches.
- Das Passwort darf keinen Begriff bilden, der in irgendeinem Wörterbuch (auch Fremdsprachen) enthalten ist.
- Verwenden Sie bei den Buchstaben eine Kombination von Groß- und Kleinschreibung.
- Passwort nicht notieren. (Kleine Zettel mit dem Passwort am Monitor oder unter der Tastatur sind keine gute Idee).
- Passwörter niemals per Mail senden, da diese Verbindungen meistens unverschlüsselt sind und die Daten im Klartext übertragen werden.
- Halten Sie Ihr Passwort geheim, es darf nicht weiter gegeben werden oder von einer anderen Person benutzt werden, bei der Eingabe sollte man auch darauf zu achten, dass man nicht beobachtet wird.
- Nach Möglichkeit sollten sensitive (root) Passwörter auch in regelmäßigen Abständen geändert werden.
- Passwort aus Anfangsbuchstaben eines Merksatzes bilden. (Es sollte so beschaffen sein, dass es schnell und blind eingegeben und dabei von anderen Personen nicht erfasst werden kann.)

Beispiel:
!1Pw=ig!
(Merkregel: !Ein Passwort ist immer geheim!)
- Das selbe Passwort sollte nicht bei verschiedenen Dienstleistern verwendet werden.

ZID password guidelines

- Das Passwort sollte mindestens 8 Zeichen lang sein und aus einer Mischung von Buchstaben, Ziffern und Satz- oder Sonderzeichen bestehen.
 - Verwenden Sie **keinesfalls** Ihren Benutzernamen oder anderen Namen (wie z.B. Vor- oder Nachname) oder Informationen, die in unmittelbarem Zusammenhang mit Ihnen stehen, wie Geburtstag, Telefonnummer, Sozialversicherungsnummer, Ausweisnummer, Autonummer, Hausnummer, Wohnort, Straße usw.
 - Benutzen Sie keine Buchstaben, die in Ihrer Muttersprache (oder in anderen Sprachen) enthalten ist.
 - Das Passwort darf keine Wörter (in beliebiger Schreibweise) enthalten.
 - Verwenden Sie bei der Eingabe keine Tabulatoren.
 - Passwort nicht notieren (z.B. auf Zettel, Karte, Postkarte, Brief, E-Mail, etc.).
 - Passwort vom Adressmanager setzen lassen ☒
 - Passwörter niemals per E-Mail, Fax, etc. übertragen.
 - Halten Sie Ihr Passwort geheim, und lassen Sie es nicht an andere Personen weitergeben. Wenn Ihr Passwort einer anderen Person benutzt werden, bei der Eingabe sollte man auch darauf zu achten, dass man nicht beobachtet wird.
 - Nach Möglichkeit sollten sensitive (root) Passwörter auch in regelmäßigen Abständen geändert werden.
 - Passwort aus Anfangsbuchstaben eines Merksatzes bilden. (Es sollte so beschaffen sein, dass es schnell und blind eingegeben und dabei von anderen Personen nicht erfasst werden kann.)
- Beispiel:
!1Pw=ig!
(Merkregel: !Ein Passwort ist immer geheim!)
- Das selbe Passwort sollte nicht bei verschiedenen Dienstleistern verwendet werden.

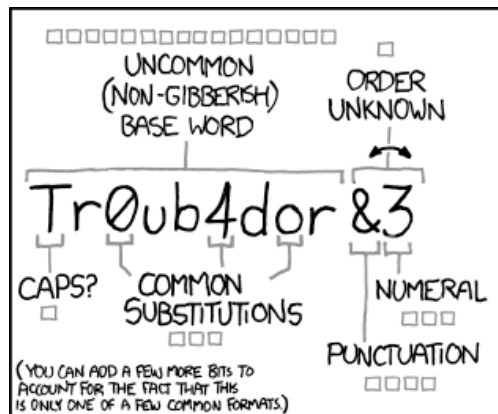
Altes TU-Passwort

Neues TU-Passwort

Bestätigung

Passwort vom Adressmanager setzen lassen ☒

Reset OK



~28 BITS OF ENTROPY

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

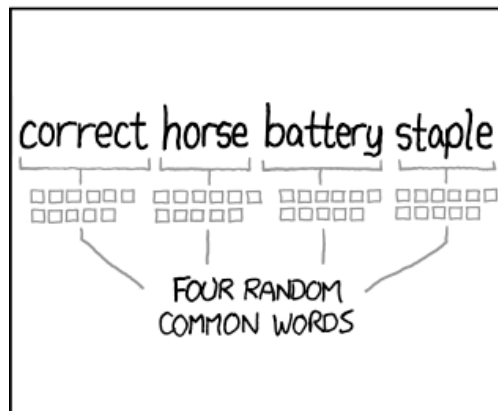
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE O's 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

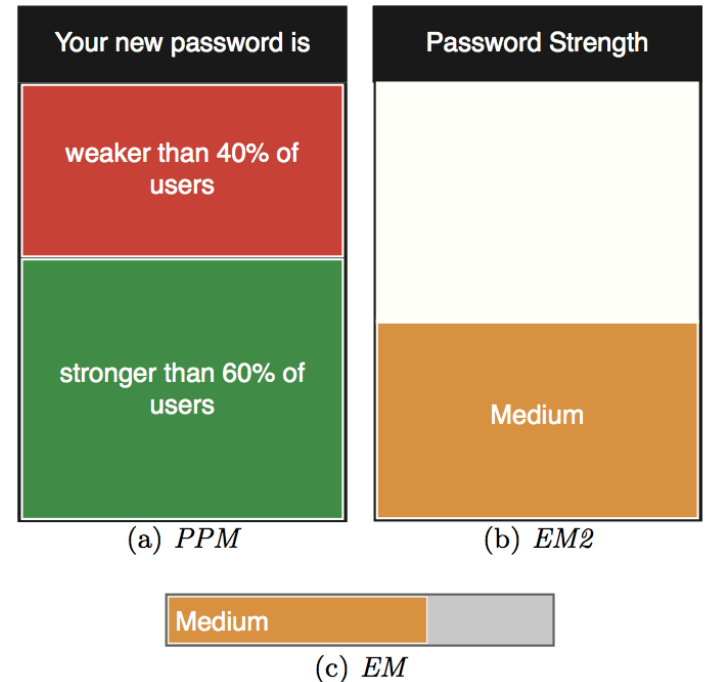
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Password checker

| correcthorsebatterystaple | | |
|---------------------------|-----------------------------------|-----|
| Services | Strength scores | |
| Apple | Weak | 1/3 |
| Dropbox | Great! | 5/5 |
| Drupal | Fair | 2/4 |
| eBay | <i>Too Long (6-20 Characters)</i> | 0/5 |
| FedEx | Very Weak | 1/5 |
| Google | Strong | 5/5 |
| Intel | Congratulations! | 2/2 |
| Microsoft (v1) | Weak | 1/4 |
| Microsoft (v2) | Strong | 3/4 |
| Microsoft (v3) | Strong | 3/4 |
| PayPal | Lame | 1/4 |
| QQ | Weak | 2/4 |
| Skype | <i>Too Long (6-20 Characters)</i> | 0/3 |
| Twitter | Perfect | 6/6 |
| Yahoo! | Weak | 2/4 |
| Yandex | OK | 4/4 |
| 12306.cn | Dangerous | 1/3 |

2013: Serge Egelman

- Lab Experiment
- 47 participants, were not aware of password test
- 2 meter types: „weak-medium-strong“ and peer pressure meter



Results

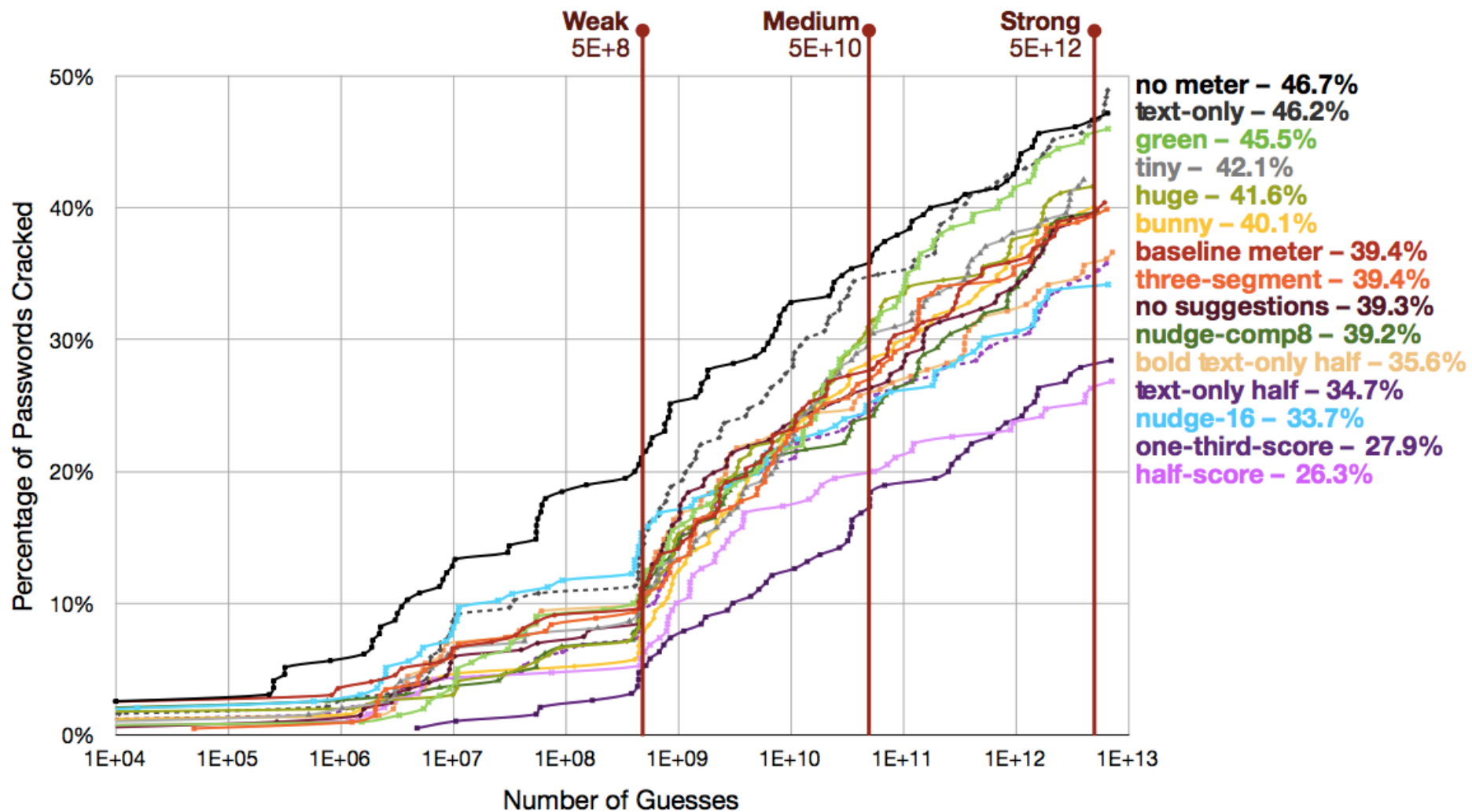
- Both meters better than none
 - Traditional meter: $p < 0.001$
 - Peer pressure meter: $p < 0.008$
- No differences between standard meter and peer pressure meter
- Password strength measured in bits of entropy

Field test

- 200 participants
 - Password for an unimportant account (survey)
- Passwords not stronger because of the context of an unimportant account

2012: Blase Ur (USENIX)

- Guess number calculator
 - 2931 participants
 - 14 meter variations: differences in text, graphic and even spinning cartoon characters
-
- Increased password length
 - More digits and symbols (on stringent meters)
 - All meters made the passwords less predictable



Comparison

- 11 password strength meters from popular web services
- Tested against common password dictionaries:
 - Cracking tools „John the Ripper“ (JR) and „Chain & Abel“ (CA)
 - Top500 (T5)
 - Conficker worm (CF)
 - RockYou (RY)
 - phpBB (PB)
 - Own L33t-dictionary (LT)
 - Mangled version of all others (*M)

| | |
|---|---------------|
| ■ | Top500 (T5) |
| ■ | Cfkr (CF) |
| ■ | JtR (JR) |
| ■ | C&A (CA) |
| ■ | RY5 (RY) |
| ■ | phpBB (PB) |
| ■ | Top500+M (TM) |
| ■ | Cfkr+M (CM) |
| ■ | JtR+M (JM) |
| ■ | RY5+M (RM) |
| ■ | Leet (LT) |



- Hybrid password checker (client and server side)
- Inconsistency („testtest“ is weak, „testtest0“ is strong, „testtest2“ is good)

Passwortstärke Gut

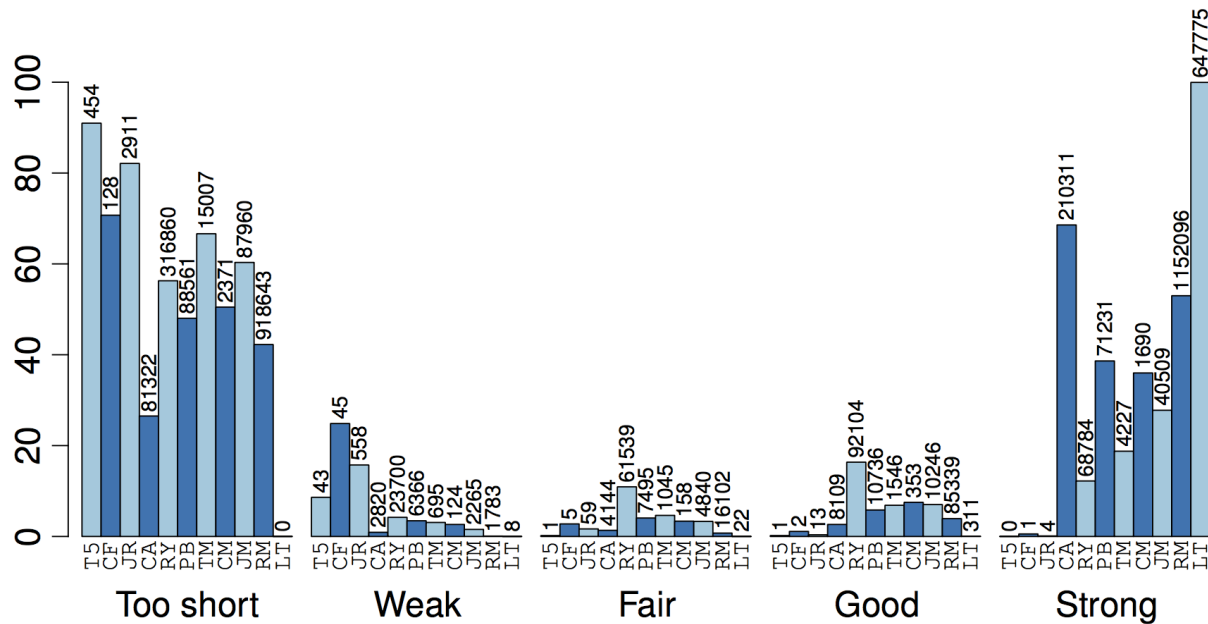
Verwenden Sie mindestens 8 Zeichen.
Verwenden Sie kein Passwort für eine andere Website oder leicht zu erratende Wörter wie den Namen Ihres Haustiers.
[Warum?](#)

Passwort erstellen

.....

Passwort bestätigen

Geburtsdatum



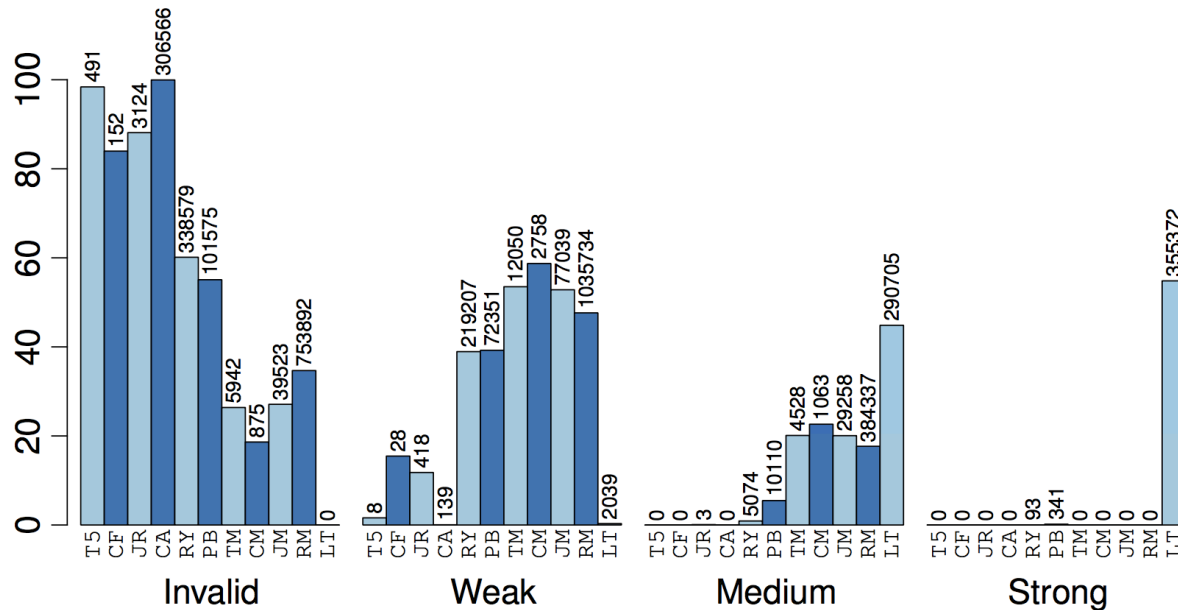


- Fully server side checker
- Very Simple (reengineered with 20 lines of javascript)
- No dictionary lookup, no l33t-transformation

..... ☐ Show

Medium

- Use 6 to 64 characters.
- Besides letters, include at least a number or symbol (!@#\$%^*-_+=&~).
- Password is case sensitive.
- Avoid using the same password for multiple sites.





- Hybrid checker
- Client side: increasing only score for upper case letters, digits or symbols
- Strict server side blacklist

.....

Passw

Sicher

Antwo

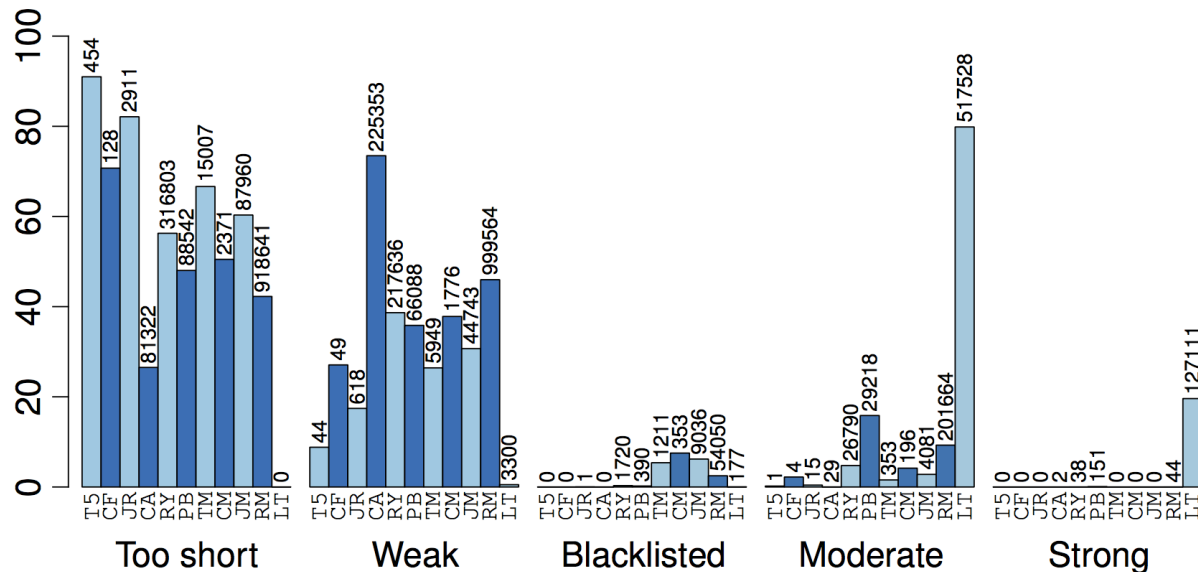
Sicher

Dein Passwort muss enthalten:

- ✓ 8 oder mehr Zeichen
- ✓ Groß- und Kleinbuchstaben
- ✓ mindestens eine Zahl

Stärke: mittel

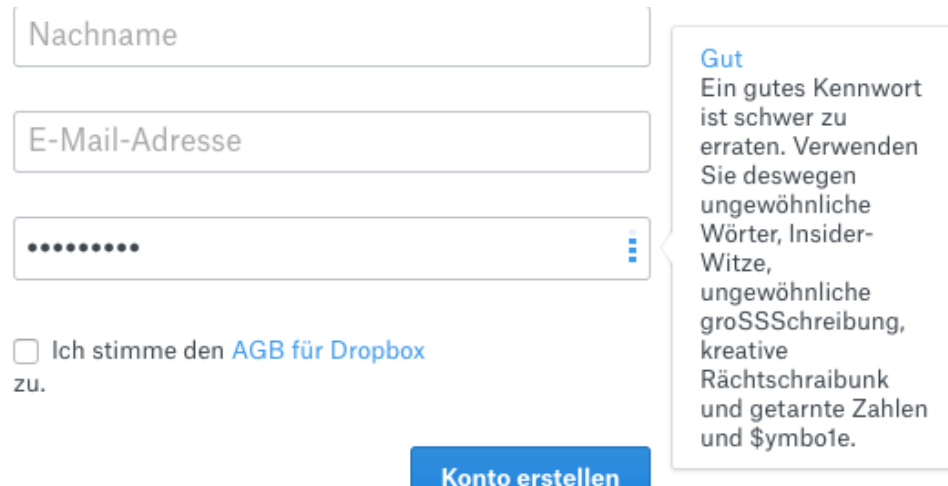
Vermeide Passwörter, die du auf anderen Websites verwendest oder leicht von anderen zu erraten sind.



Thread model

Online guessing attack

- Assume state of the art guessing algorithms
- Upper bound: 10^6 guesses



The image shows a portion of the Dropbox account creation interface. It includes three input fields: 'Nachname' (Last name), 'E-Mail-Adresse' (Email address), and a password field represented by dots. Below the password field is a checkbox labeled 'Ich stimme den [AGB für Dropbox](#) zu.' (I agree to the [Terms of Service for Dropbox](#)). A blue button labeled 'Konto erstellen' (Create account) is at the bottom. A callout box on the right provides a password strength hint.

Nachname

E-Mail-Adresse

.....

☐ Ich stimme den [AGB für Dropbox](#) zu.

Konto erstellen

Gut
Ein gutes Kennwort ist schwer zu erraten. Verwenden Sie deswegen ungewöhnliche Wörter, Insider-Witze, ungewöhnliche groSSSchreibung, kreative Rächtschraibunk und getarnte Zahlen und \$ymbo1e.

Zxcvbn - Core

Minimum rank over top lists

Input: schwarenthorer

Top passwords

1. password
2. 12345678
3. qwerty
4. 111111
5. dragon
6. baseball
7. abc123
8. 123456789
9. 12345
10. secret

Top surnames

1. li
2. khan
3. Smith
4. johnson
5. jones
6. maier
7. huber
8. davis
9. schwarenthorer
10. koch

Call-specific list

1. TU
2. Wien
3. yannick
4. schwarenthorer
5. Technische
6. Universität
7. Security
8. TUWEL
9. TISS
10. ZID

Zxcvbn - Core

Minimum rank over top lists

Input: schwarenthorer

Top passwords

1. password
2. 12345678
3. qwerty
4. 111111
5. dragon
6. baseball
7. abc123
8. 123456789
9. 12345
10. secret

Top surnames

1. li
2. khan
3. Smith
4. johnson
5. jones
6. maier
7. huber
8. davis
- 9. schwarenthorer**
10. koch

Call-specific list

1. TU
2. Wien
3. yannick
- 4. schwarenthorer**
5. Technische
6. Universität
7. Security
8. TUWEL
9. TISS
10. ZID

Output: 4 guesses

Word transformations

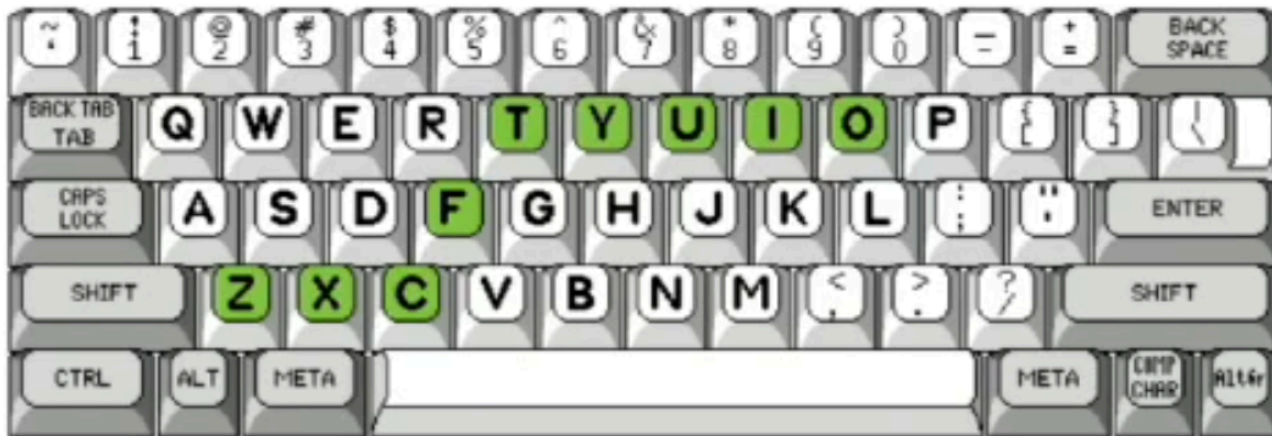
L33t: p@ssw0rd → password

capitalization: pAsSwOrd → password

reversed: drowssap → password

Keyboard patterns

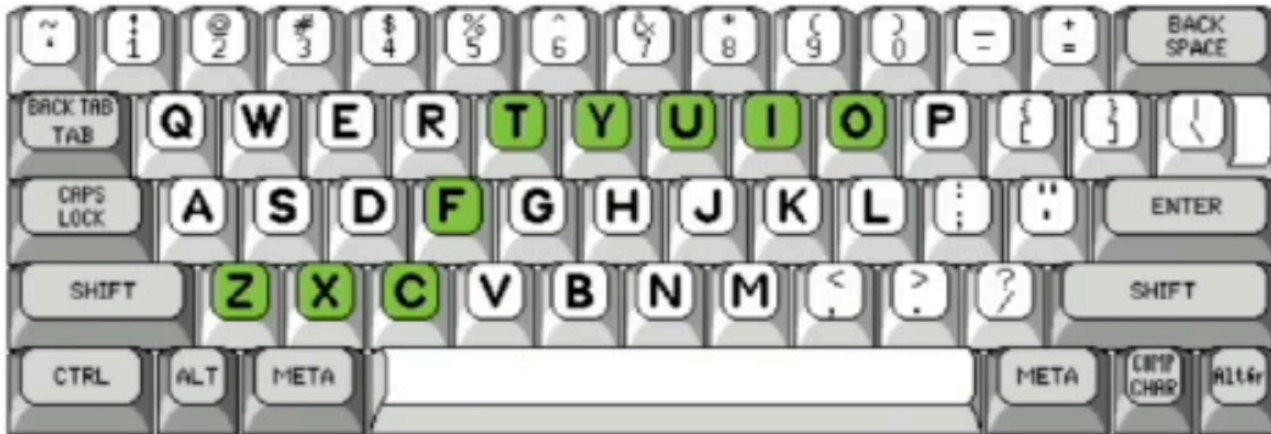
Input: zxcftyuio



Layout=QWERTY, length=9, turns=3

Keyboard patterns

Input: zxcftyuio



Layout=QWERTY, length=9, turns=3

Output $\approx 10^6$ guesses

| pattern | examples |
|--------------------|--|
| <i>token</i> | logitech l0giT3CH ain't parliamentarian 1232323q |
| <i>reversed</i> | DrowssaP |
| <i>sequence</i> | 123 2468 jklm ywusq |
| <i>repeat</i> | zzz ababab l0giT3CHl0giT3CH |
| <i>keyboard</i> | qwertyuio qAzxcde3 diueoa |
| <i>date</i> | 7/8/1947 8.7.47 781947 4778 7-21-2011 72111 11.7.21 |
| <i>brute force</i> | x\$JQhMzt |

Match → Estimate → Search

Input: lenovo2222

Match → Estimate → Search

Input: lenovo2222

| | |
|--------|---------------|
| lenovo | (password) |
| eno | (surname) |
| no | (english) |
| no | (reversed on) |
| 2222 | (2/2/2022) |
| 2222 | (repeat) |

Match → Estimate → Search

Input: lenovo2222

| | | |
|--------|---------------|---------------|
| lenovo | (password) | 11007 guesses |
| eno | (surname) | 3284 guesses |
| no | (english) | 11 guesses |
| no | (reversed on) | 18 guesses |
| 2222 | (2/2/2022) | 2190 guesses |
| 2222 | (repeat) | 48 guesses |

Match → Estimate → Search

Input: lenovo2222

| | | |
|--------|---------------|----------------------|
| lenovo | (password) | 11007 guesses |
| eno | (surname) | 3284 guesses |
| no | (english) | 11 guesses |
| no | (reversed on) | 18 guesses |
| 2222 | (2/2/2022) | 2190 guesses |
| 2222 | (repeat) | 48 guesses |

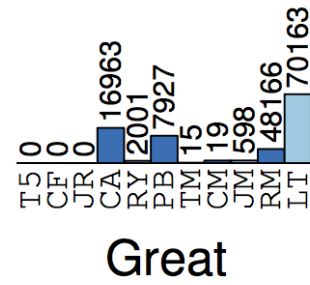
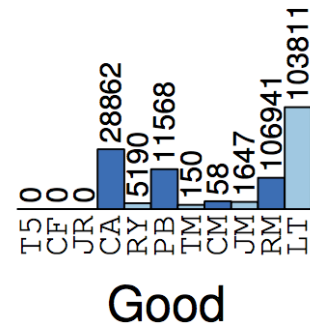
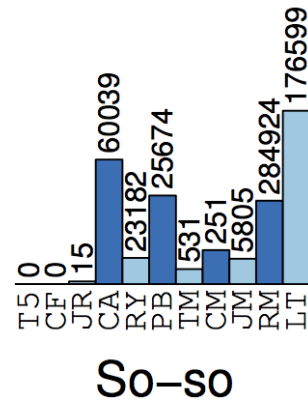
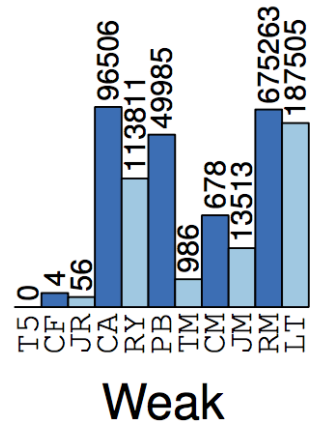
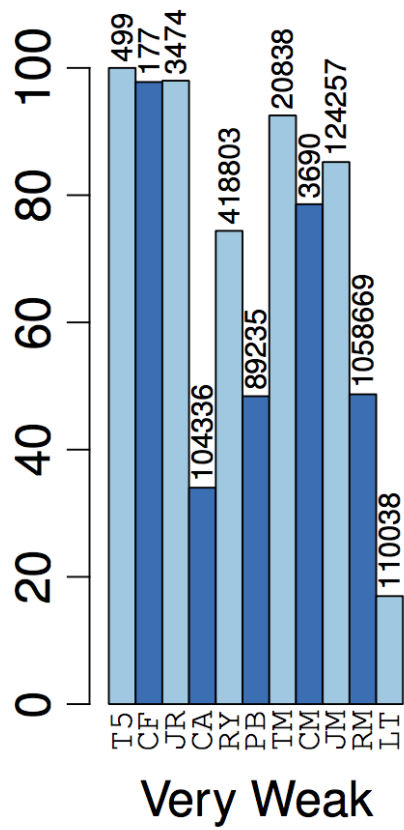
Output $\approx 10^6$ guesses

Facts

- Runs in 0.5ms in average
- Easy to use in javascript

```
var zxcvbn = require('zxcvbn');  
var meets_policy = function(password) {  
    return zxcvbn(password).guesses > 500;  
};
```

- Size of module:
 - 1.52MB with 100k dictionary entries
 - 245kB with 10k entries
 - 29.3kB with 1k entries



Thank you!