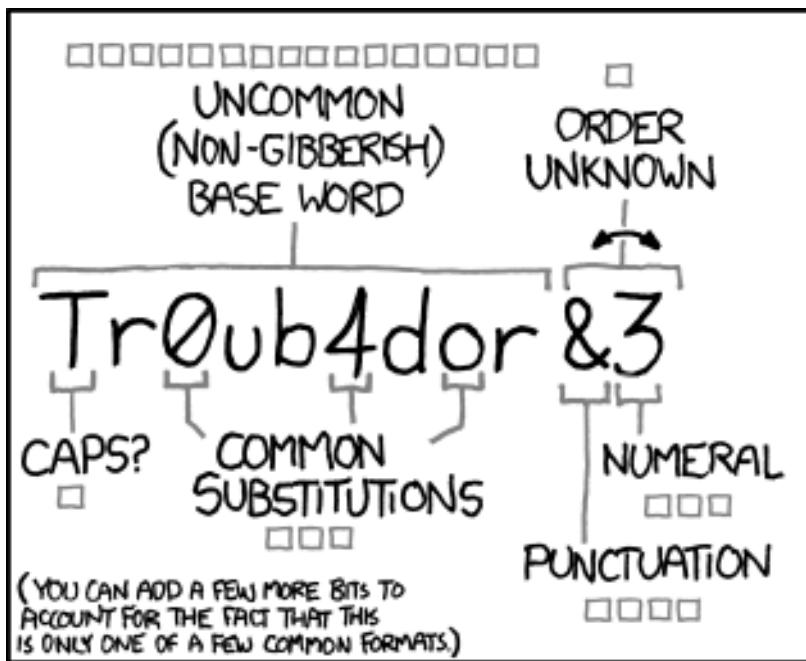


The Password Rules Horror Show

Joachim Strömbergson
Assured AB



~28 BITS OF ENTROPY

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

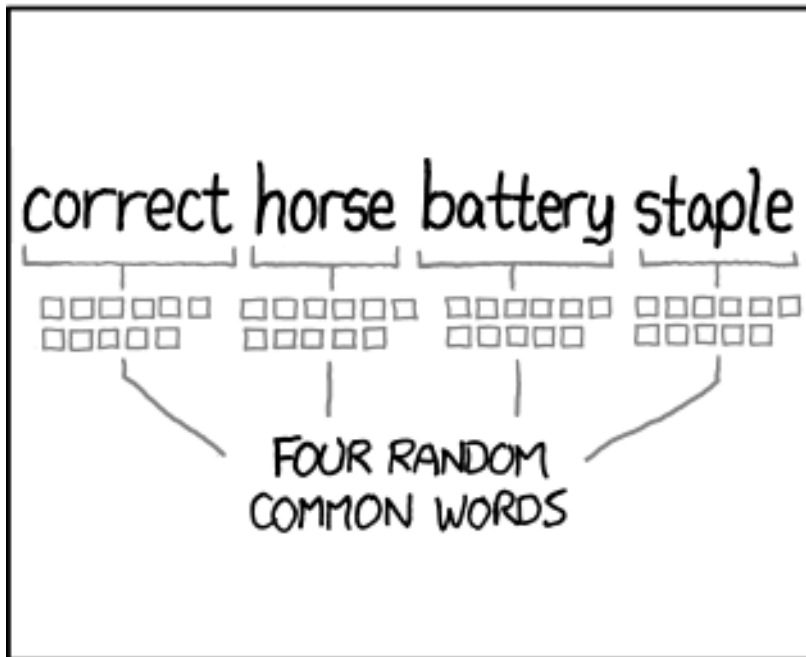
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

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

User ID and Password

- Your User ID must contain from 6 to 16 alphabetic and/or numeric characters with no spaces.
- Your Password must:
 - Contain from 8 to 16 characters
 - Contain at least 2 of the following 3 characters: uppercase alphabetic, lowercase alphabetic, numeric
 - Contain at least 1 special character (e.g., @, #, \$, %, & *, +, =)
 - Begin and end with an alphabetic character
 - Not contain spaces
 - Not contain all or part of your UserID
 - Not use 2 identical characters consecutively
 - Not be a recently used password

Password requirements: For your security, we require *strong and difficult-to-guess* passwords.

Your password will be rejected if it does not meet the following criteria. It must:

- be exactly 8 characters;
- use both upper- and lower-case letters;
- include at least one number and/or punctuation mark (allowed symbols are: ! # \$ @ _ + , ? [and]);
- contain no more than 2 numbers;
- **not** include your name or <ED: University ID>; and
- **not** appear in any English dictionary.

Your password must conform to the following format:

- Be 6 - 12 characters in length
- Contain letters and numbers only (no special characters like !,\$,*,&, etc.)
- Must contain at least 1 number
- Must contain at least 4 letters
- Cannot be your Social Security Number or email address.

Password Advisor ?

- ✗ Requires 1 numeric (0-9)
- ✗ Requires 1 alpha (a-z)
- ✗ Must include at least one special character (e.g. !@#\$%^&). First character cannot be ? or !
- ✗ Passwords cannot contain identical consecutive characters e.g. Pizza, table99
- ✗ Choose a password between 5 and 8 characters

America Express (2010)

The length of the password is limited to 8 characters to reduce keyboard contact. Some softwares can decipher a password based on the information of "most common keys pressed".

Therefore, lesser keys punched in a given frame of time lessen the possibility of the password being cracked.

Set a maximum password age of 70 days. Setting the number of days too high provides hackers with an extended window of opportunity to crack the password. Setting the number of days too low might be frustrating for users who have to change their passwords too frequently.

<http://windows.microsoft.com/en-us/windows/change-password-policy-settings#1TC=windows-7>

Bra forskning: <https://www.cl.cam.ac.uk/~rja14/shb10/angela2.pdf>



Thanks to the XKCD comic, every password cracking word list in the world probably has correcthorsebatterystaple in it already.