The Password Rules Horror Show
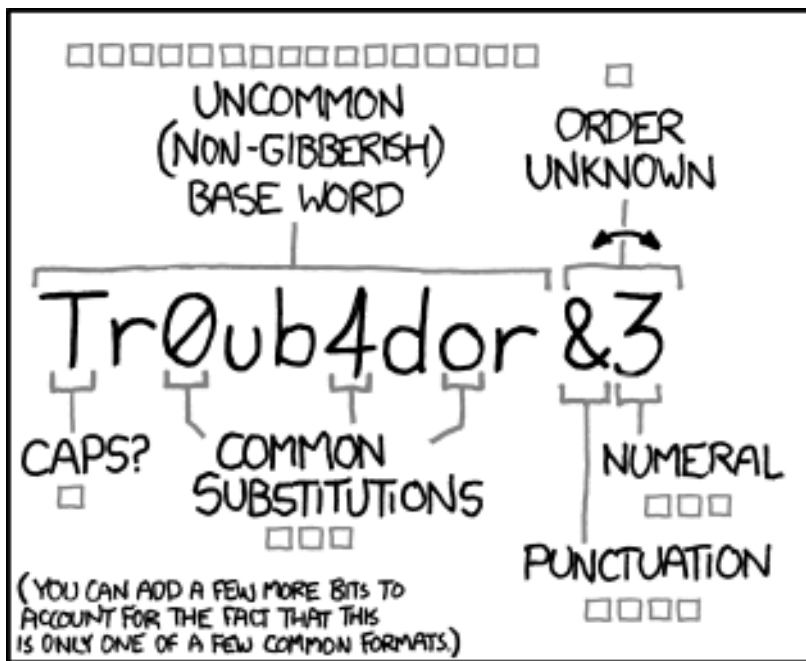
Joachim Strömbergson
Assured AB

We enforce password rules onto users
in order to improve the strength of the passwords.

Unfortunately, the research of what constitutes
good password rules are severely lacking. Instead
everyone and their cat invent their own rules for
their service. Bad rules.

This of course makes the users not only confused
but also reduces the trust in security mechanisms.

This presentation tries to collect confusing,
illogical and bad password rules.

Panel 1:

UNCOMMON (NON-GIBBERISH) BASE WORD

ORDER UNKNOWN

Tr0ub4dor &3

CAPS?

COMMON SUBSTITUTIONS

NUMERAL

PUNCTUATION

(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)

Panel 2:

~28 BITS OF ENTROPY
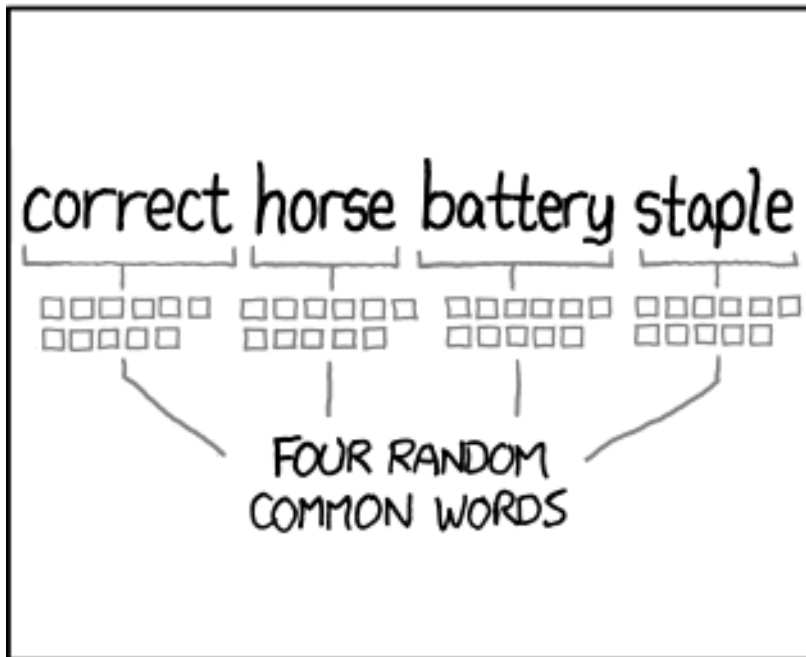
2^{28} = 3 DAYS AT 1000 GUESSES/SEC

(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

Panel 3:

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

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER:
HARD

Panel 4:

correct horse battery staple

FOUR RANDOM COMMON WORDS

Panel 5:

~44 BITS OF ENTROPY

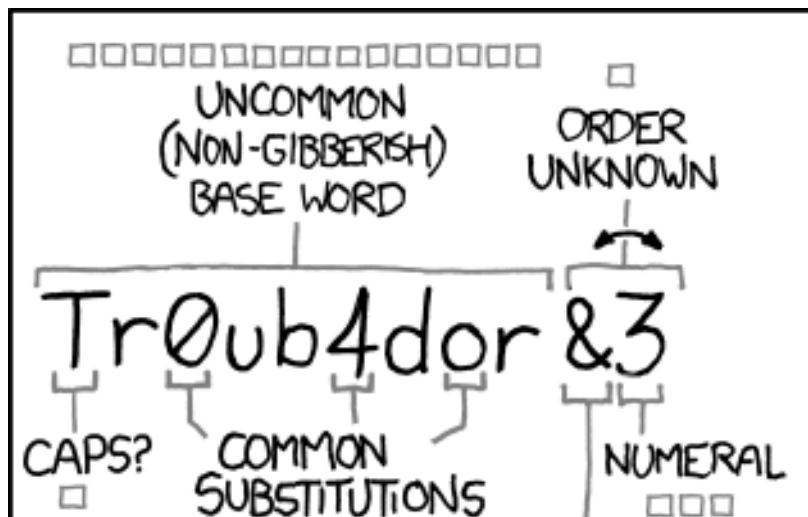2^{44} = 550 YEARS AT 1000 GUESSES/SEC

DIFFICULTY TO GUESS:
HARD

Panel 6:

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.

TRY TO USE THIS STRATEGY ON A WEBSITE WITH PASSWORD RULES

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 ⑦

❌ Requires 1 numeric (0-9)

❌ Requires 1 alpha (a-z)

❌ Must include at least <u>one special character (e.g. !@#$%^&)</u>. First character cannot be ? or !

❌ Passwords <u>cannot contain identical consecutive characters e.g. Pizza, table99</u>

❌ Choose a password <u>between 5 and 8 characters</u>

American 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.

http://www.troyhunt.com/2011/01/whos-who-of-bad-password-practices.html

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

Password Recommendations

- The password should be 8 to 63 ASCII characters long, and it is highly recommended to use 16 or more.
- Characters that are upper case. ASCII is categorized as Alpha and Numeric characters.
- DO choose each letter or digit at random. Try one-finger typing with your eyes closed.
- DO use a longer password, and write it down somewhere safe. A short password is easier to remember, but also guess. It is OK to password so you don't have to remember it.
- DO NOT use anything directly related to you, such as your street address, phone number or car license plate.
- DO NOT use the name of any person or place in your password. The attackers know all the common names.
- DO NOT use any word from the dictionary. The attackers have dictionaries, too.
- DO NOT use a phrase or sentence. Once an attacker learns any portion of the phrase or sentence, the rest is easily guessed.

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