

PASSWORTSCHUTZ

ABER WIE ?

Cryptoparty Stuttgart



CC BY-SA 4.0:
Julia Fiedler,
Thomas Christinck

18 MILLIONEN GESTOHLENE E-MAIL-PASSWÖRTER

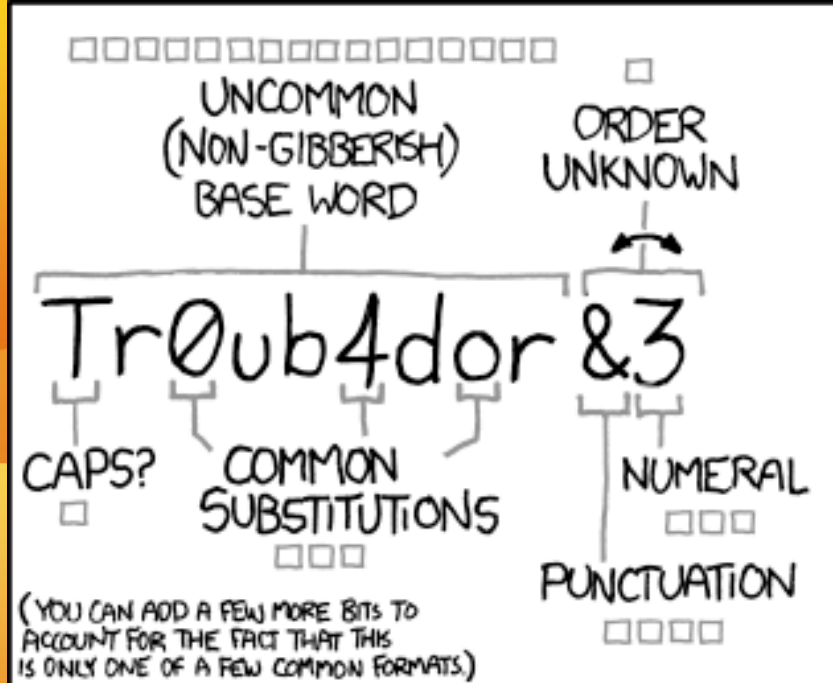
- ◆ Größter bekannter Datendiebstahl in Deutschland.
- ◆ Alle großen deutschen E-Mail-Provider betroffen.
- ◆ Die Kriminellen haben auch Zugriff auf soziale Netzwerke oder Shoppingportale, sofern mehrfach das selbe Passwort verwendet wurde.

ALLGEMEINE REGELN

- ♦ Für jeden Dienst ein eigenes Passwort nutzen
- ♦ Passwörter zufällig wählen (generierte Passwörter)
- ♦ Passwörter sicher aufbewahren.
- ♦ **Kontrollfragen für Passwörter nie wahrheitsgemäß beantworten.**

PASSWÖRTER

- ♦ Passwörter sollten mindestens acht (10/12?) Zeichen lang sein.
- ♦ Passwörter sollten immer aus Buchstaben Zahlen und Sonderzeichen bestehen.
- ♦ Passwörter sollten keine Rückschlüsse auf wichtige Daten (Geburtsdatum usw.) enthalten
- ♦ Passwörter nicht mehrfach verwenden.



~28 BITS OF ENTROPY

□□□□□□□□
□□□□□□□□ □
□□□ □□□
□□□□ □


$2^{28} = 3 \text{ DAYS AT}$
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.)

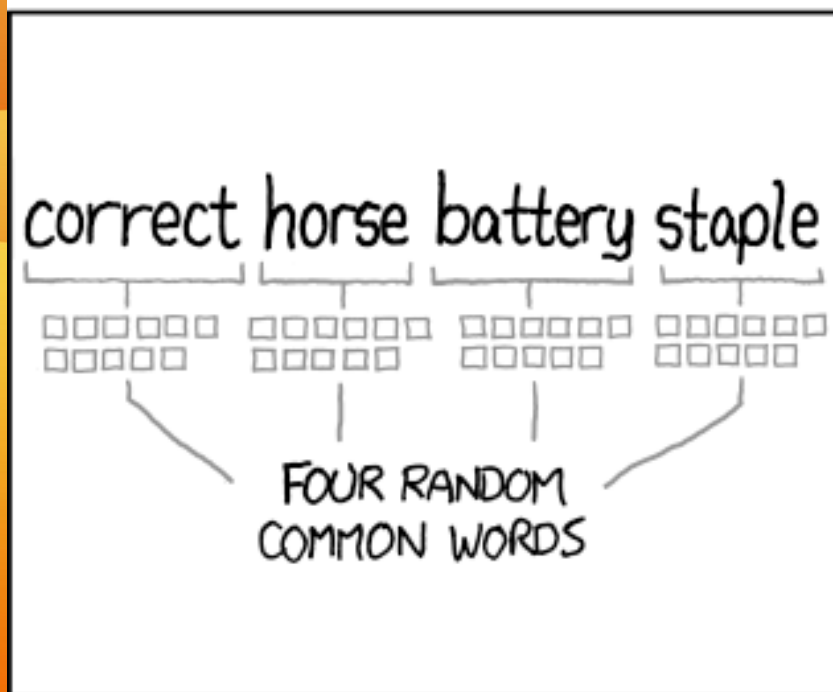
DIFFICULTY TO GUESS:
EASY

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

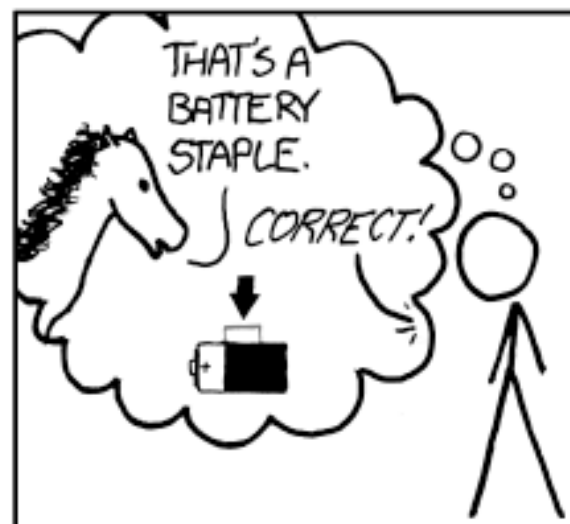
□□□□□□□□□□
□□□□□□□□□□
□□□□□□□□□□
□□□□□□□□□□

$2^{44} = 550 \text{ YEARS AT}$
1000 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.

EIGENE MERKBARE PASSWÖRTER

- ◆ Eigenes Schema ausdenken um von einer Vorlage andere Passwörter ableiten zu können.
- ◆ **Beispiel:**
- ◆ 1 und 3 Buchstabe der Internetseite an drittletzter und letzter Stelle der Passwortvorlage einfügen.
- ◆ Anzahl der Buchstaben an zweiter Stelle einfügen.

EIGENE MERKBARE PASSWÖRTER

- ♦ Passwortvorlage: 2X:Bt784X
- ♦ Website: www.webmontag.de (9Buchstaben)
- ♦ Passwort: 209X:Bt78w4Xb
- ♦ Erster Buchstabe an drittletzter Stelle
- ♦ Dritter Buchstabe an letzter Stelle
- ♦ Niemals genau dieses Schema benutzen, sondern ein eigenes Schema ausdenken.
- ♦ Ein allgemein bekanntes Schema macht Passwörter vorhersehbar und eventuell knackbar

❓ **GENERIERTE PASSWÖRTER**

- Ein generiertes Passwort wird zufällig erstellt.
- Passwortlänge und Komplexität kann bestimmt werden.
- Generierte Passwörter können nicht ohne weiteres geknackt werden.
 - - KeePass (Linux, Windows)
 - - Passwörter über Schlüsselbundverwaltung generieren (MacOS)

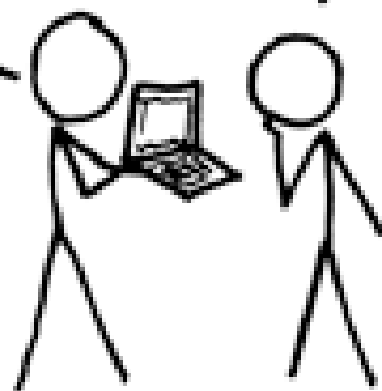
NERDS !!

A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

BLAST! OUR
EVIL PLAN
IS FOILED!

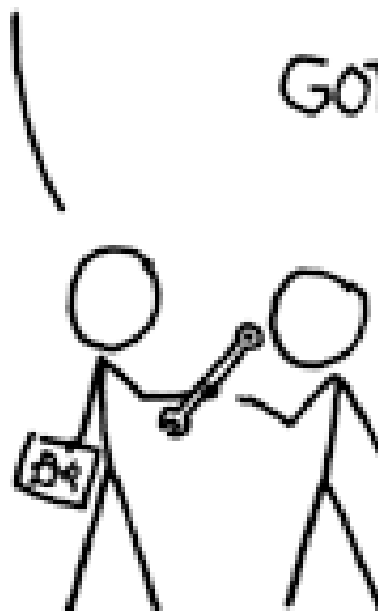
NO GOOD! IT'S
4096-BIT RSA!



WHAT WOULD ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

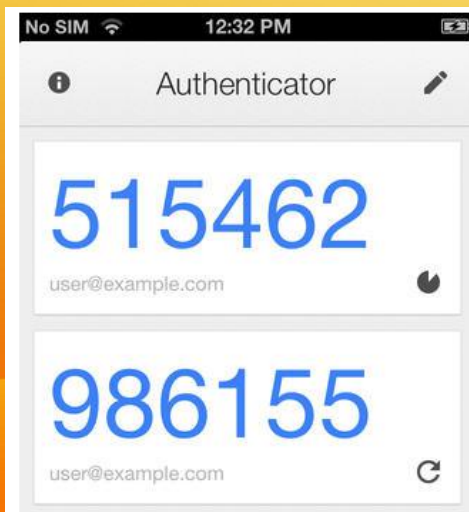
GOT IT.



ZWEIFAKTOR-AUTENTIFIZIERUNG (2FA)

ONETIME PASSWORD (OTA)

- ◆ Außer Username und Password noch ein **weiteres** Password aus einer **zweiten** Quelle
- ◆ Beispiel: TAN beim Onlinebanking
- ◆ Beispiele: Google Authenticator, Yubikey, verschiedene Open Source Lösungen incl Pebble-App



ZWEIFAKTOR-AUTENTIFIZIERUNG (2FA)

ONETIME PASSWORD (OTA)

- ♦ Aber was ist bei Verlust des Generators?
 - ♦ Recovery ?
- Backup der Seeds (Startpassworte)

VIELEN DANK

FRAGEN?