# A \d+ Minute Introduction to Diceware

https://github.com/rlindsgaard/presentations/tree/master/cryptohagen/diceware

---

Ronni Elken Lindsgaard
rel@zx.dk
@rlindsgaard

2017-02-026

# What is Diceware?

A method for creating passphrases, passwords, and other cryptographic variables using ordinary dice as a hardware random number generator.[1]

[1] https://en.wikipedia.org/wiki/Diceware

# A brief history lesson

- Arnold Reinhold - 1995[2]
- EFF - 2016[3]
- Multitude of localised versions including Danish and Esperanto.

[2] https://en.wikipedia.org/wiki/Diceware

[3] https://www.eff.org/deeplinks/2016/07/new-wordlists-random-passphrases

# What you need

- A word list[4]
- A 6-sided die (or 5 preferably)
- Pen and paper

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

# Word list

```
...
24642 elaborate
24643 elastic
24644 elated
24645 elbow
24646 eldercare
24651 elderly
24652 eldest
24653 electable
...
```

# The Password Generation Algorithm - 1

Roll the five dice all at once (or one 5 times consecutively) and note down the facing sides (without looking at the wordlist!). Repeat 5 times.

```
2, 4, 6, 4, 5
6, 1, 5, 5, 1
6, 2, 5, 3, 3
1, 2, 1, 1, 6
3, 4, 2, 1, 4
6, 2, 3, 3, 3
```

# The Password Generation Algorithm - 2

Look each corresponding word up in the word list.

```
2, 4, 6, 4, 5 elbow
6, 1, 5, 5, 1 tacking
6, 2, 5, 3, 3 triage
1, 2, 1, 1, 6 antarctic
3, 4, 2, 1, 4 humorist
6, 2, 3, 3, 3 tilt
```

# The Password Generation Algorithm - 3

Write it down, using a memnonic you will remember

I hurt my **elbow** on a **tacking** under the **triage** in the **antarctic**a when the **humorist** **tilt**ed on his leg.

# Special Characters, Numbers, and Concatenation

- Concatenation: elbowtackingtriageantarctichumoristtilt, elbow tacking triage antarctic humorist tilt, elbow1tacking2triage3antarctic4humorist5tilt
- 3lb0w t4ck!ng tr!@g3 4nt@rct!c huJVLor!$t t!1t

# Security discussion

- Word list contains $6^5 = 7776$ words
- Each word adds $log_2(6^5) = 12.9$ bits of entropy
- Use least six words (77 bits entropy)[5]
- Use client-side generators only.
- Do not change the order, keep it truly random.
- Do not ever re-use your passwords!

[5] https://arstechnica.com/information-technology/2014/03/diceware-passwords-now-need-six-random-words-to-thwart-hackers/

# Just Because

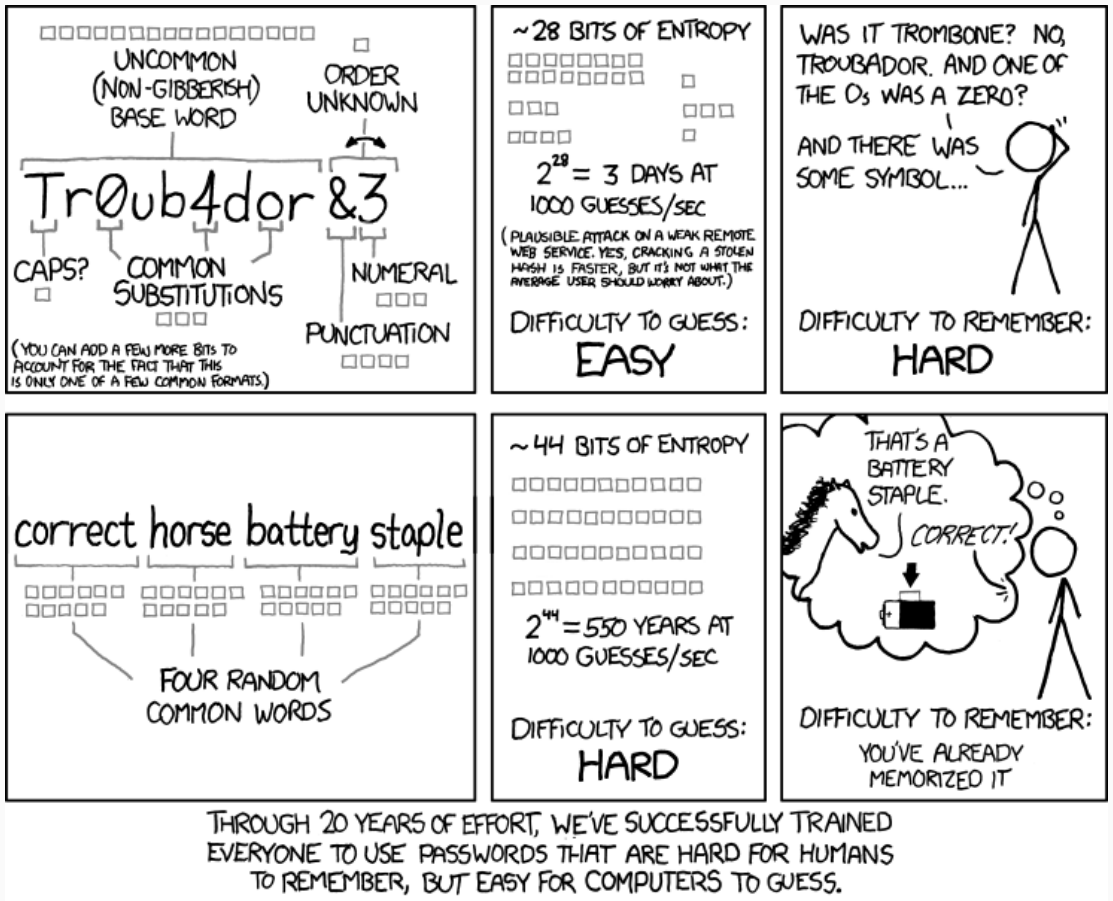


**Figure 1:** https://www.xkcd.com/936/

# Do You Want to Learn More?

- https://www.eff.org/dice
- https://ssd.eff.org/en/module/animated-overview-how-make-super-secure-password-using
- http://world.std.com/~reinhold/diceware.html

# Questions?

Questions?