IDPro Body of Knowledge - Demo

Principal Editor: TBD

September 28, 2018

Contents

1 Authentication 1

1.1 Passwords 1

1.1.1 Entropy 1

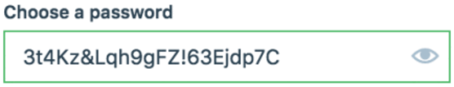
1.2 One Time Codes 1

1.3 One Time Pad 2

1 Authentication

1.1 Passwords

This section is about passwords. The length of the password helps the security but makes it hard to remember



Choose a password

3t4Kz&Lqh9gFZ!63Ejdp7C

Figure 1: A strong (but) static password

1.1.1 Entropy

You may recall from high school physics that entropy has something to do with thermodynamics. Why in the world is it used to describe passwords?

Claude Shannon coined the use of the term “entropy” in information theory when he recognized the formula he had developed for measuring information also occurred in statistical mechanics, where it was called entropy! He used the letter H to represent it since it was so in Boltzmann’s famous H theorem, which has to do with molecules moving to equilibrium.

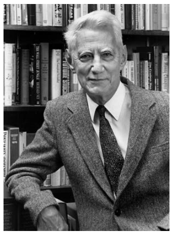


Figure 2: Claude Shannon

For passwords “Entropy” denotes the uncertainty in the value of a password.

Entropy of passwords is conventionally expressed in bits, which brings you back to high school math. That’s right logarithms! If your alphabet consists of 26 letters, say and you require 8 letters in your password then there are 26^8 possible passwords. That can be expressed as entropy with

$$H = \log_2(26^8) = 37.6 bits$$

More information is provided by NIST at `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf`.

Humans don’t do random very well, so in reality, much of the possible space is never taken by self-selected passwords, so in practice the entropy is overstates the value.

Of course, modern computers with access to the password hash file can make quick work of this. So finding ways to prevent or throttle password guessing is important! Or, better yet, don’t rely entirely on passwords!

1.2 One Time Codes

This section is about codes that can be only used once. Of course the problem with codes that can be used just once is that there is a distribution problem. In earlier times, this was solved by creating a codebook with two copies - one for the sender and one for the receiver. In modern times there are time based codes, that depend on minimizing the difference between local clocks.

1.3 One Time Pad

Here is an example of a one time pad

```
ZDXWWW EJKAWO FECIFE WSNZIP PXPKIY URMZHI JZTLBC YLGDYJ
HTSVTV RRYYEG EXNCGA GGQVRF FHZCIB EWLGGR BZXQDQ DGGIAK
YHJYEQ TDLCQT HZBSIZ IRZDYS RBYJFZ AIRCWI UCVXTW YKPQMK
CKHVEX VXYVCS WOGAAZ OUVVON GCNEVR LMBLYB SBDCDC PCGVJX
QXAUIP PXZQIJ JIUWYH COVWMJ UZOJHL DWHPER UBSRUJ HGAAPR
CRWVHI FRNTQW AJVWRT ACAKRD OZKIIB VIQGBK IJCWHF GTTSSE
EXFIPJ KICASQ IOUQTP ZSGXGH YTYCTI BAZSTN JKMFXI RERYWE
```

Figure 3: A one time pad