Why Choosing the Right Password Matters

Revision 2

Databases storing account credentials get compromised

Adobe - **153 million accounts**
LinkedIn - **6.46 million accounts**
RockYou! - **32 million accounts**
Playstation Network - **77 million accounts**
Yahoo! - **453,000 accounts**

These databases are analyzed (due to poor implementation or brute-force attacks) and the results are used to further enhance cracking methods.

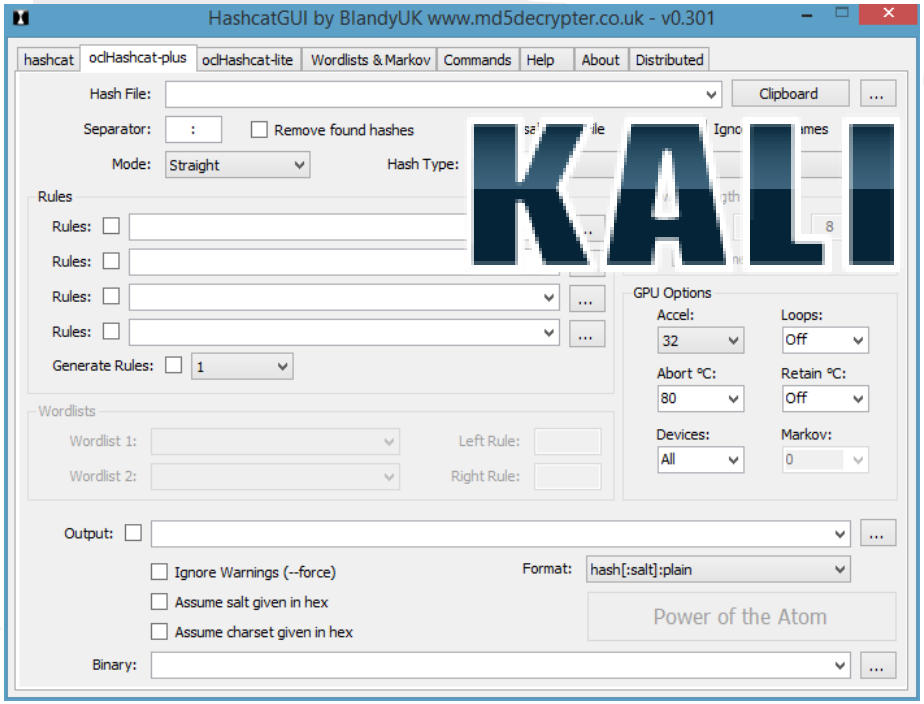
So how easy is it to crack passwords?

Modern hardware including many-core CPUs, GPUs, and cloud computing make it more feasible to crack a passwords (and derivations thereof) in a *reasonable* amount of time.

CloudCracker

Continued...

Software to leverage modern hardware is freely available and often very easy to use. Large dictionaries are easily procurable via BitTorrent.



KALI LINUX

Case in point...

Example attack on a wireless router using WPA encryption:
Hashed password was extracted by listening to wireless packets, locating a client and "bumping" them from the network forcing a new authentication exchange.
The first attempt took two hours using a dictionary attack (30GB dataset) with no results. Using the same dataset common combinations were added (numbers before and after the word, etc.) returned a nine character alpha numeric result in 40 minutes.

This leads to the question...

Do I use the same or similar password for everything?

People tend to use the same password (or a slight derivation), **for every service they use!**

Using the password from the prior slide, could it be used to login to their router? How about the user's computer? Their Facebook account? E-mail account?

How can I defend against this?

Don't use anything related to you that can be found out easily (address, phone number).
Don't use sentences from anything that can be searched electronically.
Do use special characters: ~!@#$%$^&*()-+
Do make them more than 8 characters in length.
Don’t use the same password twice.
Do use software such as Lastpass to help.
Do use passphrases.
Do use 2 factor authentication.

Choosing an effective password

Randomly generated passphrase:
total proper three mood
Randomly generated password:
1^7Tp#1&jb&DWZ7rWmN&bCQeD$

Random matters! Do not try and randomly create your own password, humans are terrible at it. (http://bit.do/dt9c)

Use a service such as Lastpass with a passphrase and generate long random passwords for everything else.

Tools

Generate passphrases:
https://www.xkpasswd.net
https://en.wikipedia.org/wiki/Diceware

Check your password strength:
http://rumkin.com/tools/password/passchk.php

Lastpass
http://www.lastpass.com
KeePass
http://keepass.info/

Defense in depth

Adding an additional layer of authentication will *drastically* increase the difficulty!

If you have the ability to turn on two factor authentication, **DO IT**. The trade-off of more time to authenticate is worth it!

Questions to ask yourself

- Do I use the same password for multiple services (including debit card pins, car entry, etc.)?
- Do I use simple (short) passwords?
- How often do I change my passwords?
- Has my password already been compromised?
- Do I use 2 factor authentication when available?
- Do I share my passwords with others?

THE END

(now go forth and change your password)