Usage

Lauri Kangassalo

June 16, 2013

Brief instructions

Starting the program will launch a text-based user interface. The program will prompt you to select all sorts of things, but in case you don't know any of this mumbo jumbo about chains and tables, here's a quick way to test the program:

1. Find the program in the root of the github repository
2. Choose to generate a rainbow table with the following attributes: lowercase alphanumeric character set, min and max password lengths: 4, chains per table: 420000, chain length: 2000
3. Wait for the program to finish, and run it again, this time choose the option Crack an MD5-hash
4. Load a rainbow table named: 36-4-4-420000-2000.tbl
5. Start cracking your alphanumeric passwords of the length four!

Note! The *threaded* version of the software has a slightly better UI.

Advanced instructions

There is a lot to play with the software. By changing the attributes, you can crack passwords up to 8 characters of length. In theory. I have never tried it, since I haven't got the time to generate rainbow tables so large.

The greatest problem comes when one needs to decide on the chains per table and chain length values. More chains per table mean bigger table files and more collisions, since same starting points are generated randomly. More chain length affects performance greatly, and also adds to the risk of chains colliding. On the other hand, if the two values are too small, not all of the chosen character set's keyspace is covered, meaning that the plaintext for a hash won't be found in any of the chains. The UI will give some hints for these values, but they are highly experimental. The only way to find out the correct parameters is to try.