Cracking User Passwords

By Stephen Jones

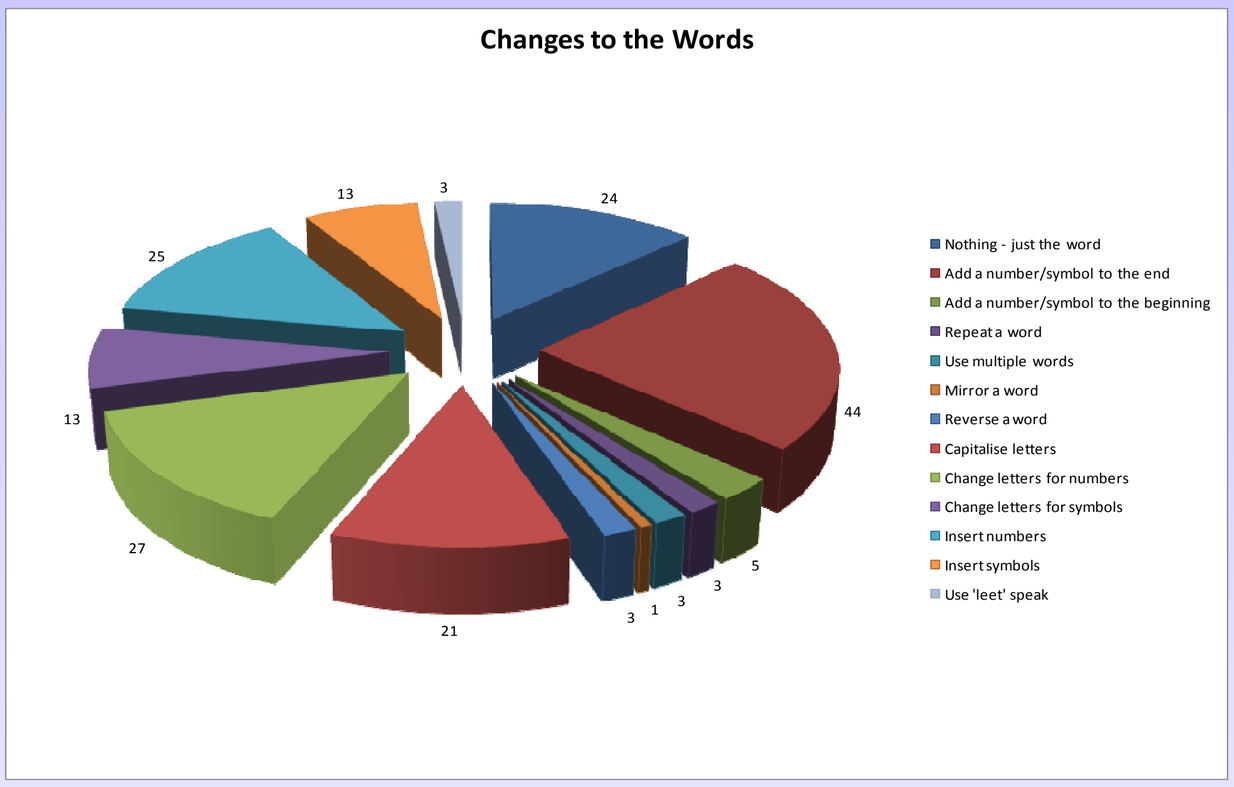
Motivations:

Passwords have become a necessary part of everyday life, being the most common way users authenticate and log-on to websites. Passwords therefore need to be memorable for the user and secure.

Forcing users to use a mixture of lower case letters, upper case letters, numbers and symbols is commonly used by companies to help to ensure security of passwords. Does this actually work?

Password Generation Methods:

Research has shown people commonly generate a password by choosing a word and making changes to it:



The question then is:

Do changing words in these ways actually make more secure passwords?

Implementation:

A program was written which took 5 of these methods and tried to crack as many passwords as possible from a list of 244 SHA-1 hashes of old user passwords.

The methods used were:

- **Words on their own**
- **Words followed by letters**
- **Words followed by symbols**
- **Words with letters changed for numbers or symbols**
- **Words with numbers and symbols inserted**

A brute force attack was also implemented but only run on passwords up to 5 characters long as longer than this would take too long to run. The estimate for a brute force attack on a 6 character password is about 150 days!

Running the Program:

The program ran for 2 weeks during which it cracked about one quarter of the 244 passwords.

For comparison JohnTheRipper, a well known open source password cracking program, cracked about 20 more passwords in the 2 week period.

Examples of Passwords Cracked:

password albert! hello2 smith tripleh 10011982 fen1x 1111 banana342 pop91 fhtn cH41ana 15117d yellow6 hello v10l3t 2307 drowssap ryan muigy65 torres gacko hljeb chothia purple74 engage7052 prolog68 hello11111 sparkle55 spooky01 vera8859 kribicka

Conclusion:

Any password which is generated by choosing a word and changing it through a set of rules is a bad way to create a password because as shown a program could be created which follows the same set of rules to crack the password.

Secure Password Generation:

To generate a secure password, a random string of letters, numbers and symbols would be best, but this is not going to generate a memorable password for the user.

Memorable Password Generation:

To generate a memorable password which is also secure it is recommended that users start with something which is not a dictionary word and then change it in a number of ways. For example take the first letters from the words of a phrase or a line from a song, then change letters for symbols or numbers. For example:

Don't Stop Me Now Cause I'm Having A Good Time

gives:

dsmncihagt

changing letters gives:

Ds39ci#aG+

which when tested for 2 weeks was not cracked.

This password is still created using rules, but as there are so many phrases which could be used and it would be difficult to make a list of all of them, this decreases the probability the password will be cracked.