CALIFORNIA STATE SCIENCE FAIR
2008 PROJECT SUMMARY

Name(s)
Marie E. Nielsen

Project Number
S1317

Project Title
Is Safe Good Enough? The Value of Added Complexity in Password Security

Abstract

Objectives/Goals
The objective of this project is to predict the ability of brute force password decryptors to decode passwords, then compare the predicted decoding times with experimental results.

Methods/Materials
Password lists were created for multiple character ranges and lengths, encoded as Unix passwords and then decoded. Predicted decoding times were compared with experimental results. Predicted password decoding times were proportional to the number of possible character combinations, and was calculated from the number of guesses per second, number of bytes in passwords, character types used in passwords. A personal computer, password lists, and opensource software was used. For each experiment 20 random passwords were encrypted. The time to decode 20 passwords using exhaustive guessing was recorded. Statistical analysis compared predicted versus actual results. For each experiment, a password list was created for a specific character range and length.

Results
The amount of time predicted to decode passwords exponentially increases as the length and character choices in a password increased. A high correlation was shown to exist between the predicted and actual time measured to decode the passwords. The exponential relationship between complexity and time to decode can be extrapolated to determine how large a random password must be to be safe.

Conclusions/Discussion
Through the course of predicting data, collecting data, and analyzing the data, certain relationships and patterns were seen. A highly correlated relationship appears to exist between password length and the time (seconds) it takes to decrypt as well between the character set employed and the time to decrypt. Shorter, less complex passwords, even when encrypted, can take mere seconds to be decrypted. When these results are considered in light of real passwords, the patterns in real passwords that people select themselves allow the passwords to be more vulnerable to decoding.

Summary Statement
Predicting password decryption based on combinatorics.

Help Received
My parents helped explain statistical and encryption concepts, Paul Roth for usage of the UCSC library.