CALIFORNIA STATE SCIENCE FAIR
2017 PROJECT SUMMARY

Name(s)

Anna V. Orgel

Project Number

J1506

Project Title

The Relationship between Password Characters and Guesses Required Using a Self-Developed Brute Force Hacking Program

Abstract

Objectives/Goals

This study measured the variation in number of guesses required for different types of passwords using a brute-force program I created and modified on scratch, a computer coding website.

Methods/Materials

Materials: Laptop computer with self-developed Scratch program, online character randomizer (Random Letter Sequence Generator: www.dave-reed.com)

Used a website to generate random passwords of a given length and create lists of 25 passwords for each category containing various numbers and types of characters. Compared average number of guesses required for each type of password using self-developed Scratch program. This program was created by modifying an existing program on Scratch that determined password strength. The modifications I made were:

1) Expanded the original program into seven categories for each type of password;
2) Changed the variables and lists to match those within each category;
3) Added a counter to display total number of guesses required for each password;
4) Added function to allow user to choose designated password character category before entering password.

Number of guesses for each password were recorded and averages taken for each category. Averages were then compared to a previously predicted number based on the formula: number of possible characters^digits.

Results

The results of the study showed a positive, exponential relationship between the number of possible characters and the average number of guesses required. The passwords with more possible characters were most secure, and the passwords with fewer possible characters were less secure. The results closely matched the predicted values using the formula: number of possible characters^digits. My hypothesis was supported.

Conclusions/Discussion

Every decade we become more reliant on technology, but as we become more adept at using it, hackers threaten to compromise our security. My study and the ease with which my program guessed passwords confirms the necessity of higher level security precautions for computers other than passwords. Furthermore, it demonstrates the overall fallibility of passwords, especially given our human tendency to select those that are most easy to remember, and therefore most easy to hack.

Summary Statement

My study examined the relationship between the number and type of characters in a password and how easily they were guessed by a program that I developed using Scratch, a programming website.

Help Received

The program was developed completely independently, excluding minor bug checking help from my math tutor. The experiment was performed with no help, and the write up was only briefly edited by a parent.