Password cracker: a test of the reliability of passwords for online security

Ivaylo Krumov
BSP 1 - BiCS Semester 1 (2021-2022)
ivaylo.krumov.001@student.uni.lu

Project objectives

The purpose of this project is to analyze and assess the reliability of passwords - the most commonly used defense in online account security. The project will consist of two different parts. One part will focus on scientific research, through which the main question of the project will be answered, while in the other part a program will be developed, which will give an answer to the main question in a practical and visual way. Although they will be very distinct from one another in terms of functionality, each part will complement the other when answering the main scientific question. The results and answers that will be produced from both parts will be compiled together so that the quality of the final assessment will be as high as possible. The project is expected to give insight into the level of security that different kinds of passwords are able to provide for users' accounts. It will also aim to help the reader understand what the most common reasons for vulnerable passwords are and suggest some existing effective ways of preventing passwords from being easy victims of cracking algorithms.

Prerequisites

The complete realization of the project, both the scientific and the technical part, will require the possession of several skills and competencies. The following is a list of all the abilities that are already known before the beginning of work for this project and are related to its scientific part:

- Understanding the purpose and importance of passwords for online security;
- Comprehending information from scientific sources;
- Writing well-structured pieces of work.

Respectively, these are the skills that are already in possession before any implementation of the technical part of the project has started:

- General experience with programming using the Python programming language;

- Preparedness for improvement and optimization of long and complex code.

These prerequisites, in combination with the additional knowledge obtained during the work on the project, will be used to fully develop both parts of the project.

Project description

Scientific description

Main scientific question: **How reliable are passwords for online security?**

This question will be answered by a method of analysing scientific papers that deal with finding answers to similar topics. For reference, a total of 6 papers will be used, listed below by order of relevance:

1. Viktor Taneski, Marjan Heričko, Boštjan Brumen, “**Systematic Overview of Password Security Problems**”, Acta Polytechnica Hungarica, Vol. 16, No. 3, 2019
2. Katha Chanda,"**Password Security: An Analysis of Password Strengths and Vulnerabilities**", International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.7, pp.23-30, 2016.DOI: 10.5815/ijcnis.2016.07.04
3. Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Rich Shay, Tim Vidas Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Julio Lopez, “**Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms**”, CMU-CyLab-11-008, August 31, 2011
4. Blase Ur, Jonathan Bees†, Sean M. Segreti, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, “**Do Users’ Perceptions of Password Security Match Reality?**”, CHI 2016
5. Elda Kuka, Prof. Assoc. Dr. Rovena Bahiti, “**Information Security Management: Password Security Issues**”, Academic Journal of Interdisciplinary Studies, Vol 7 No 2, July 2018
6. Shannon Riley, “**Password Security: What Users Know and What They Actually Do**”, Usability News, Vol. 8 Issue 1, February 2006

The first four pieces of work are fully-fledged and well-structured academic articles that go into great detail about the research each of their authors has done, while the rest simply show the results of independent surveys, but are nevertheless just as useful because of the data they contain. The first three of these papers will be considered as main references and will therefore be utilized the most for answering the scientific question. The most relevant information from all articles will be collected and synthesized in order to form a proper scientific answer to the question.

In order to properly give an answer to the scientific question, the question itself will be split into three smaller-sized questions, those being:

- What is reliability?
- What is a password?
- What is online security?

These questions will be answered using information from the three main articles, with some support from the secondary articles wherever it is suitable. All main papers contain some forms of answers to the first and third question, while sufficient information regarding the second one can only be found in the second main paper. If necessary, the three sub-questions will additionally be split into more questions in order to find a properly defined answer to each of them. The final answer of the main scientific question will be compiled from all the answers to all defined sub-questions.

Technical description

A Python program will be created that will attempt to gain access to a specific external file. This file's contents will be protected by a password, which the user will be prompted to input upon program execution. The maximum length of the password will be explicitly stated. The entered password and its length will then be stored in variables. Based on the user's input, the program will check what set of characters it will need to use for the cracking process. Only after going through these preparations will the program finally be ready for use.

Following the preparation phase, the program will allow the user to interact with a simple graphical user interface. This GUI will consist of a displayed time limit, a timer and a button, which upon click will start, stop or reset the current program attempt. Upon clicking the start button, the program's cracking algorithm, which will be based on the brute-force password cracking technique, will begin executing. It will generate numerous possibilities for character strings with the length of the password, while also taking into consideration the set of characters that was chosen in the preparation phase (for different passwords this set may have different properties such as containing numbers, having both lower- and uppercase letters, or the inclusion of special characters). Each generated string will be checked against the actual password until a correct match is generated. After a correct guess, the program will stop and access to the file will be unlocked. At any point during the code's execution, the user will have the option to stop the process manually by clicking the stop button. After the code has finished executing, the user will be able to click the reset button if he/she wishes to do the same attempt again.

During the string generation, the GUI's timer will also be running. Once the program stops, the timer will do too. Its value will then be checked against the displayed time limit, which will act as a success condition. If the program manages to generate the correct password within the time limit, then this will be counted as a successful cracking attempt, and unsuccessful otherwise.

The entirety of the program will be written in the Python programming language. Additionally, the planned graphical user interface will be created with the help of the PySimpleGUI Python package. The GUI will be implemented in such a way that the user will be able to interact with it upon the execution of the program. The main algorithm of the program will work based on the user's interaction with the GUI itself, meaning that the user will be able to directly choose from the GUI whether to run the code or terminate its execution.