JRC-PaStMe Readme

JRC-PaStMe is a tool allowing user to assess the strength of their password. Its approach is different from most of the available one that generally rely to the NIST specification. This latest is based on construction rules (e.g. minimum length, presence of capital letters, presence of special characters and digits…). Our approach relies on four different modules each of them assessing different characteristics of the password therefore embracing the different strategies used by malicious people when they try to retrieve users' passwords.

Installation

Decompress the application archive, make sure that all the required dll are within the same folder as the executable. To use the pre-trained matrices, decompress the corresponding archive and place the matrices in the same folder than the executable one.

Windows:
Simply launch the executable

Mac & Linux
Install the mono package and then use the following command in a console
mono JRC-PastMe.exe

Evaluating password strength

Two possibility are offered, either evaluating a single password getting immediate feedback or evaluating all the passwords contained in a file storing the results. The corresponding button bring you on the dedicated page.

Single Password

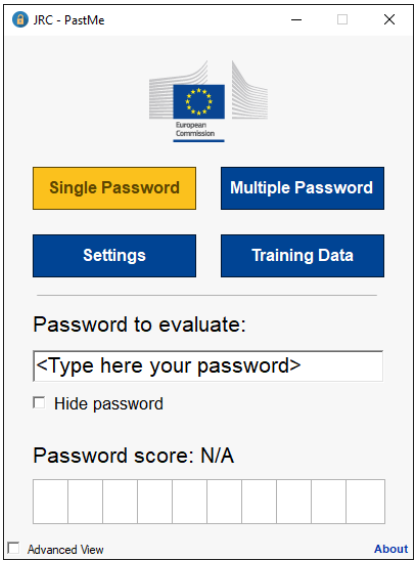

Figure 1 Standard View in Single Password Mode

Type the password to evaluate in the correct field (see Figure 1). The displayed score is between 0 and 10, 0 being weak password and 10 strong. Enabling the advanced view (see Figure 2) give you more details about the score obtained within the four different modules. By checking the box 'Hide Password', the password is hidden allowing anyone to test their own password even if someone can see the screen.

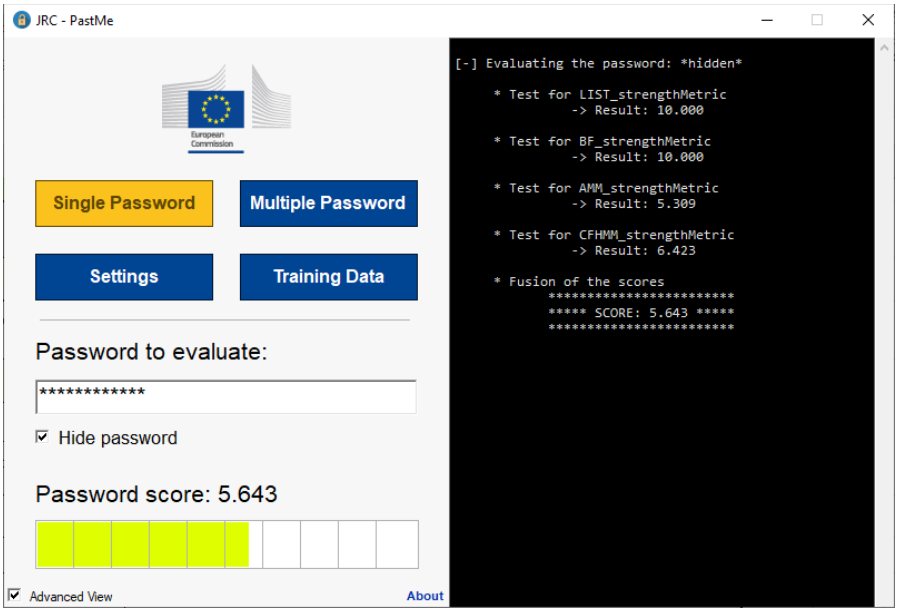

Figure 2 Advanced View in Single Password Mode

The four different modules are briefly described below, more information on them can be found in the original scientific article (DOI: 10.1109/TIFS.2016.2636092).

Exhaustive search module:

This module check whether the password is not too short according to some predefined parameter (see Section about settings below) and the type of characters used in the password (e.g. lowercase, numbers…).

Blacklist Module:

This module checks if the password is not contained in the blacklist that is a file containing *weak* passwords. Passwords relatively close, for example with a single character different, to those in the list are also considered as weak by this module.

Adaptive module and Hierarchical module:

These modules use a pre-trained matrix to evaluate if a password is following a similar construction strategy than those in the training list of password. Basically a fully random password is not following any construction pattern and would be given a good score by these modules. The difference between the two modules is how the password is analysed. One is using a sliding window of three characters and use the probability that a sub sequence of x consecutive characters of the password is followed by the next character. The other one divide the password in blocks of type of characters (block of lowercase, block of number…) and then assess each block individually.

Multiple password

Multiple passwords can be evaluated in a single action by selecting the corresponding text file from the application (see Figure 3). The text file should contain a single password per line. The results will be stored in the same folder using by default the same filename as the original file extended by "_results". The filename can be optionally modified in the corresponding text field below the button. The results are stored in a csv format facilitating the exploitation of the results. The structure used to store them is the following one:

Password, score_list, score_exhaustive, score_adaptive, score_hierarchical, final_score

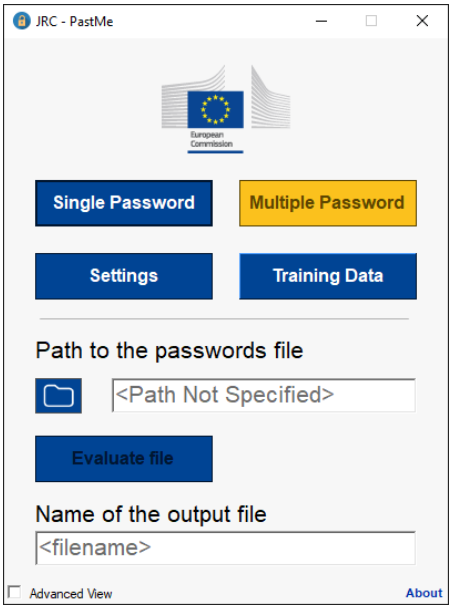

Figure 3 Standard View in Multiple Password Mode

Settings

The parameters of the two first modules (Exhaustive search and Blacklist) can be specified in this tab (see Figure 4). Default values for the exhaustive search and a default blacklist are already defined in the delivered application. The exhaustive search parameters define the minimum number of characters a password should have to be considered as strong by the exhaustive search module during the password evaluation. There exist seven different values specifying such length depending of the type of characters composing a password:

- Four in total when a password is composed solely of characters from a single class of characters (lowercase, uppercase, numbers, special)
- Three values if the password is composed of a mix of two, three or the four classes of characters.

The blacklist file used can be changed providing the path of the new file in the application. The file should be a text file where each line is a different password.

There are two available encoding that can be specified for the password to be evaluated. Either the 95 printable characters of ASCII or first one thousand characters of the Unicode character set.

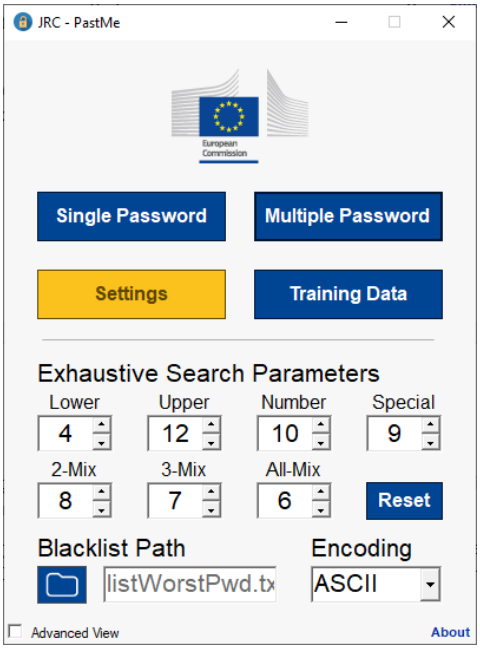

Figure 4 Settings Tab

Training

The matrices used to evaluate the password with the two last modules can be retrained with the own data of the user (see Figure 5). The selected training file should be a text file where each line contains a single password. The encoding for which the training should be performed must be selected. The two encodings can be trained consecutively by checking the two dedicated boxes. Once the training file has been selected, just click on the training button to trigger the training. Information about the training process are displayed in the advanced view console.

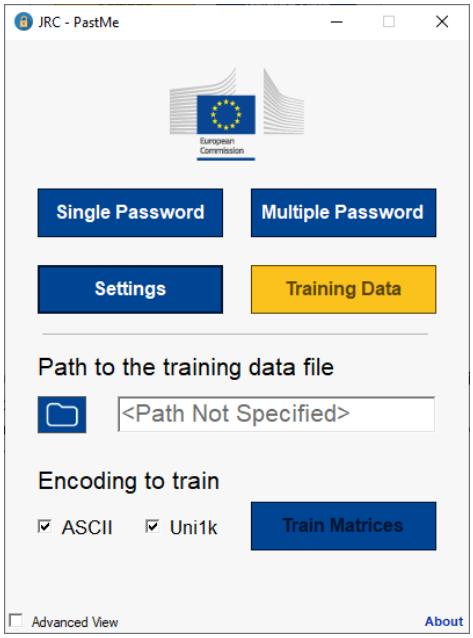

Figure 5 Training Tab