Password Complexer

Mohamed Amine Osmani

<mohamed.amine.osmani.job@gmail.com>

Table of Contents

1. Abstract.....3

2. Introduction.....3

3. Problem Statement.....4

4. Proposed Solution.....5

4.1 Introduction of Solution.....5

4.2 How Password Complexer Works.....6

4.2.1 How the user can use password complexer.....6

4.2.2 How the algorithm works.....8

4.3 Algorithm analysis.....9

4.3.1 Method of analysis.....9

4.3.2 Results.....9

4.3.2.1 Results before using password complexer.....10

4.3.2.1 Results after using password complexer.....11

5. Discussion.....12

6. Future Direction and Long-Term Focus.....12

7. Conclusion.....12

References.....14

1. Abstract

Passwords are the most important asset that we should take care of when we are online. We should use secure passwords instead of using weak passwords.

Using secure passwords in our daily life is important because it allows us to protect our accounts from hackers. Users use weak passwords all the time instead of using a secure passwords.

Password complexer is software that helps us to use secure passwords without choosing and remembering them. It takes a weak password from the user and then turns it into a secure password that the user can use. It can turn even the worst 10000 passwords into secure passwords.

Password complexer will allow us to use secure passwords without choosing and remembering them.

The next step for making the users use secure passwords is to make the algorithm behind password complexer more secure and implement it directly into the authentication system.

2. Introduction

We use passwords to log into our accounts. There are two types of passwords weak passwords and secure passwords. The vast majority of us use weak passwords instead of using secure passwords.

Weak passwords are easy to hack, guess and crack. for those reasons, users should use secure passwords, But they don’t use them because they are hard to choose and remember. And they have to remember so many secure passwords because they have a lot of accounts.

Forcing users to choose and remember secure passwords is hard, For those reasons the objective of this paper is to introduce a solution that will make users use secure passwords without choosing or remembering them. the only thing that they need to do is to remember their weak passwords.

3. Problem Statement

When it came to passwords we have a few problems:

- Users use weak passwords all the time because they are easy to remember. But those passwords cause a lot of problems. they are easy to hack, guess and crack.

- Users have to manage a lot of accounts, and with each account, they need a password. So managing and remembering a secure password for each account is a hard task.

For those reasons the proposed solution can solve those problems, and make the process of choosing and remembering secure passwords much more efficient and easy.

4. Proposed Solution

4.1 Introduction of Solution

Users are very good at choosing and remembering weak passwords, And they aren’t good at choosing and remembering a secure password. For this reason, it’s better to find a solution that turns these weak passwords into secure ones, so that the user doesn’t need to choose or remember secure passwords.

Password complexer is software that takes a weak password and then turns it into a secure password that the user can use.

4.2 How Password Complexer Works

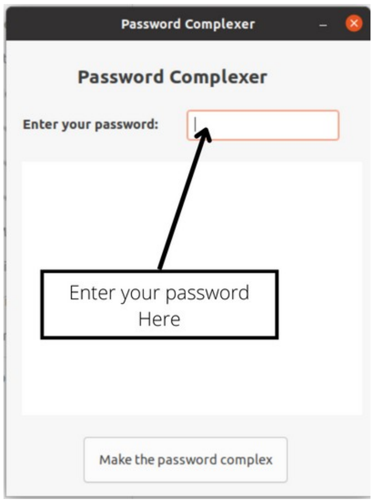
4.2.1 How the user can use password complexer

The main role of password complexer is to make users use secure passwords without choosing or remembering them.

So how to use password complexer?

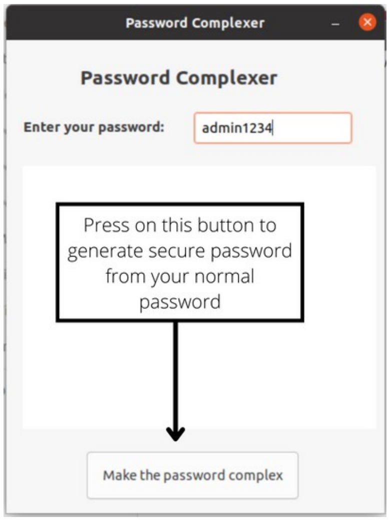
Step one

Enter your normal password into password complexer.



Step two

Press on the button so that password complexer can generate a new secure password.

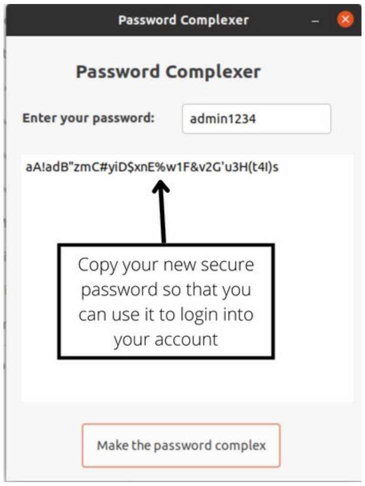


Enter your password: admin1234

Press on this button to generate secure password from your normal password

Step three

Copy your new secure password and use it.



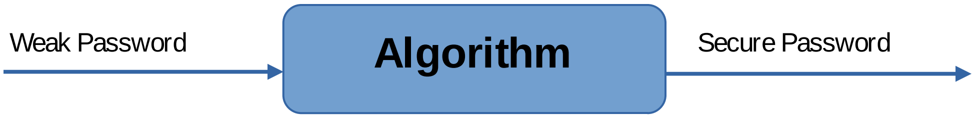
Enter your password: admin1234

aA!adB"zmC#yiD$xnE%w1F&v2G'u3H(t4I)s

Copy your new secure password so that you can use it to login into your account

4.2.2 How the algorithm works

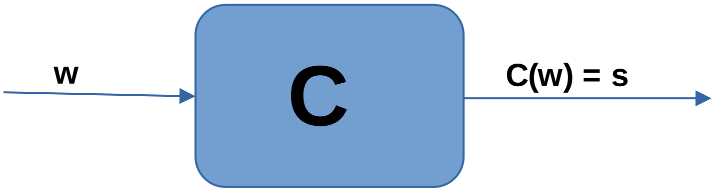
The main role of the algorithm is to turn weak passwords into secure passwords.



The algorithm takes a weak password as an input and then returns a secure password as an output.

The user gives the algorithm his weak password as an input. and the algorithm returns a secure password as an output.

The equation of the algorithm is: **C(w) = S**



C: algorithm **w:** weak password
s: secure password

4.3 Algorithm analysis

4.3.1 Method of analysis

In this analysis, I have used the list of common 10000 passwords [1]. And I have used a password strength meter [2] to calculate the strength of each password. The password meter has a scale from 0.00 to 0.99, if the strength of a password is above 0.66 then the password is secure, and if it below 0.66 the password is not secure.

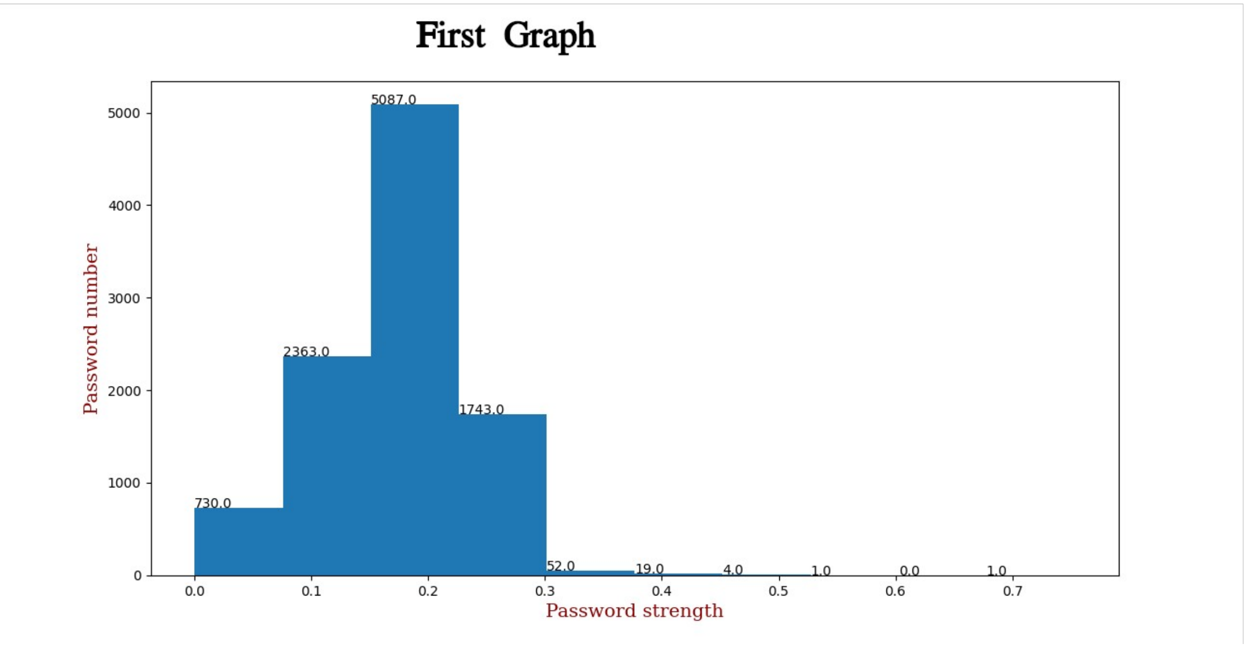
In the first analysis, I calculated the strength of each password in the list, and then plot the results in the first graph. The graph shows the strength of the passwords.

In the second analysis, I used password complexer algorithm to make the passwords more secure, and then I calculated the strength of the new passwords to see if password complexer algorithm can make weak passwords secure, and plotted the results in the second graph.

4.3.2 Results

The two graphs below show the strength of the passwords, how many passwords are secure, and how many passwords are weak passwords. The first graph shows the passwords strength before using password complexer algorithm, and the second graph shows the passwords strength after using password complexer algorithm.

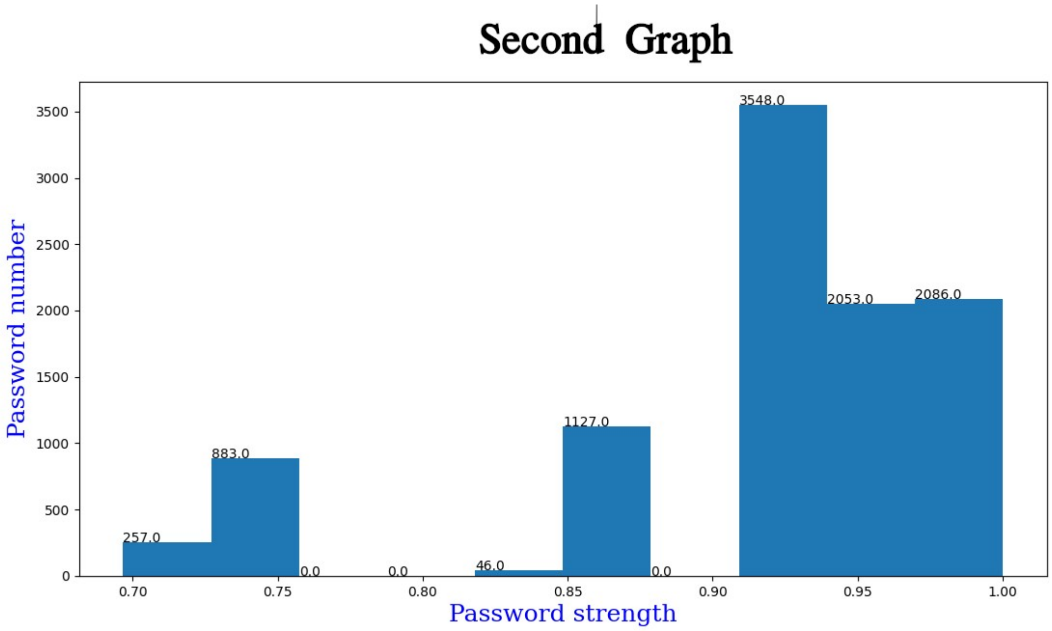
4.3.2.1 Results before using password complexer



The Fist graph shows that the vast majority of the passwords in the list have low password strength. The graph also shows that 5087 passwords have a strength between 0.1 and 0.2 this means that 50% of the passwords in the list are not secure passwords.

The results in the graph mean that passwords in the list are weak passwords because most of them have a strength below 0.66.

4.3.2.1 Results after using password complexer



The Second graph shows that after using password complexer algorithm the strength of the passwords becomes above 0.66, this means that password complexer algorithm can turn weak passwords into secure passwords.

5. Discussion

The results in the first graph and second graph show that after using password complexer algorithm on weak passwords the vast majority of the new passwords generated by password complexer are secure passwords. This means that password complexer algorithm can turn weak passwords into secure passwords.

With password complexer we can improve the strength of weak passwords that the users use without forcing them to choose and remember secure passwords.

6. Future Direction and Long-Term Focus

In the future, the main focus should be on making the algorithm behind password complexer more secure. Also, we should implement this algorithm directly in the authentication systems and browsers.

7. Conclusion

Users use weak passwords all the time because they are easy to choose and remember. But they are easy to hack, guess and crack. Users don’t use secure passwords, because they are hard to choose and remember. Using weak passwords instead of using secure passwords puts users and companies at big risk.

Password complexer is a solution that will allow users to take their weak passwords and turns them into secure passwords that they can use to log into their accounts. This solution will make the users use secure passwords all the time without choosing or remembering them.

The data shows that password complexer can turn the worse

passwords into secure passwords that the user can use instead of using his weak passwords. It will help users and companies to increase their security.

in the future the main focus should be on making users use password complexer, making the algorithm behind password complexer more secure, and implementing the algorithm directly to the authentication systems.

References

[1] P. Miessler. “SecLists/10-million-password-list-top-10000.txt at master · danielmiessler/SecLists · GitHub” Github. https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/10-million-password-list-top-10000.txt (accessed Aug. 27, 2022).

[2] M. Vartanyan. “password-strength.” The Python Package Index (PyPI). https://pypi.org/project/password-strength/ (accessed Aug. 27, 2022).