International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Password Strength Analyzer

Bhavani Gorle*

GMR Institute of Technology Razam, Kinneravada, Thogiri, Saravakota, Srikakulam, Andhra Pradesh, PIN-532427, India.

ABSTRACT

Security knowledge is one of the foremost challenges in the present day. Once a user is talking about security the primary thing that comes into the view is 'Cyber crime' which is increasing immensely day by day. Cyber Security provides the best way of protection. When a user is visiting any site it requires login credentials. Passwords are meant to gain access to specific data, an account, or a protected space. Passwords are a way to authenticate the user and thus a robust password should be carefully created. One user may have multiple accounts that are protected by password search shows that users tend to stay the same or have similar passwords for various accounts. Generally, the strength of the password is checked and supported by the overall guidelines prefer it should contain alphanumeric characters, special symbols, etc. In this study, the discussion is mainly about the various algorithms and policies to make a strong password, therefore, the strength of a password is checked through segmentation algorithms and analyses whether the chosen password is a strong password or a weak password. Passwords with less correlation of personal details are the safest to use.

Keywords: Password, Security, Hashing, Password Strength, Correlation, Entropy

1. Introduction

A password may be a secret word or string of characters that are used for authentication, to prove identity, or gain access to a resource. Password strength may measure a password's effectiveness in resisting guessing and brute force attacks. The key to a powerful password is length and complexity. Length is solely the number of individual characters utilized in the creation of the password, while complexity refers to the number of characters that would potentially be employed in the creation of the password. The strength of passwords is basic to make sure the safety of present-day frameworks, irrespective of whether or not they are near home monetary accounts, corporate servers, databases, or IoT gadgets. Here there are three segmentation algorithms are used that are maximum matching, triangular matrix, and password segmentation algorithm. the most ideal of the segmentation algorithm is to figure out this optimal solution supported by the optimal results of the last step. Here the three segmentation algorithms are compared to see the simplest password strength analyzing algorithm. Here each password is split into several meaningful words rather than the equivalent length of substring s.

2. Literature Review

- This Paper Discussed Analysing the strength of passwords through segmentation algorithms. Analyzing whether the chosen password is based on user attributes is a serious security challenge in modern systems. A password is considered to be strong if it is not based on user attributes and weak if it is based on user attributes. Many segmentation algorithms exist, namely maximum matching, triangular matrix, etc. This paper proposed an optimal segmentation algorithm for partitioning the password which provides better results than the existing algorithms. [1]
- This paper discussed about the characteristics of the user's chosen password and allowed the user to create a strong password. The most commonly used Password Encryption methods such as Hash Technologies, Password Entropy, and Password cracking algorithms are described.[2]
- The various password policies recommended by the NIST are explained such that a user can have a better understanding of how a strong password can be created. As the Password algorithm is the backend of the different websites for reflecting the password strength meter the various schemes involved in it are explained. It is also mentioned that future work involves user testing of the new password strength meter to the existing one.[2]
- This paper discusses how a password analyzer can help all organizations, from small companies to large corporations. This password analyzer works by first asking a user to enter a password with a minimum of an eight-character length. If the length falls short then it'll prompt the user to re-enter his or her password another time. Once the user enters a sound password string the program will then provide suggestions on the way to edit your current password to create a fair stronger one.[3]
- To create a powerful password the user must ensure to include: graphic symbol letters, upper-case letter letters, digits, special symbols, and a length of no but 8 characters. If the user successfully includes these 5 elements, then a malicious hacker would want to travel through 95 different possible characters for every character within the password string. There are two styles of threats, internal threats and external threats.

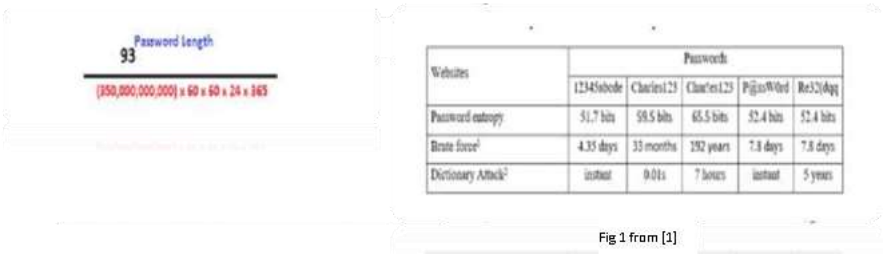
Internal threats are those threats that come from inside the organization's network while external threats and attacks come from outside an organization's network.[3]

- The main objective of this paper is to the Password Strength Estimation. The current estimation methods which are classified into three main groups: attack-based, heuristic-based, and statistical-based methods also are explained. A novel multimodal and flexible method for the estimation of password strength is described. To achieve the goal of multimodality and adaptableness, two new probabilistic methods supported by the Markov chains are proposed to accurately estimate the strength of non-trivial passwords: 1) the Markoff process with adaptive memory and 2) the Hierarchical Markov Chain.[4]
- This Paper [5] discusses the various Tests for analyzing the time taken to break the password. Numeric test - The first test run was for 5-letter passwords and then for 6-letter passwords. The time to break a single password was calculated for passwords using the various tests
    - Numeric Test
    - Alphanumeric Test
    - Multicase Test

3. Methodologies

The password cracking algorithms [1] were implemented by finding the time to crack a password in the view of password cracking attacks. The basic idea of brute-force attacks is to try to exhaustively search the entire possible password space until the correct password is found. Brute force attacks can be guaranteed to crack all the passwords, but are not feasible for very long passwords due to time and resource constraints. Compared with brute-force attacks, dictionary attacks exhaustively search all possible words in a list, which is called a dictionary; these attacks require less time and have a better attack effect than brute-force attacks, but cannot be guaranteed to crack all the passwords. The words in the dictionary are more likely to be real pa sswords. However, the password strength under a dictionary attack directly depends on whether the password is in the attacker's dictionary file. If the user modifies the original password, for example, if the password "password" is changed to "password123" or "p@sswOrd", and the modified passwords are not in the dictionary file, the difficulty of cracking passwords will increase.

- Formula to Calculate in Years, How Much Time it Would Take to Successfully Brute-Force a User's Password.



Websites	Passwords				
	12345abcde	Charles123	Charles123	P@ssWord	Re32(dqq
Password entropy	51.7 bits	59.5 bits	65.5 bits	52.4 bits	52.4 bits
Brute force[1]	4.35 days	33 months	192 years	7.8 days	7.8 days
Dictionary Attack[2]	instant	0.01s	7 hours	instant	5 years

Fig 1 from [1]

The password strength has been analyzed using the password entropy method [2] and here the Entropy is given by **H = L* log2N** ,where L is the length of the password .N is the character size. Let the password be = 'Ast34beta1' which is chosen out of a 62 size character set. Then the entropy is H= 10 * log1062/log102 . **H= 59.541.** Minimum of six and a maximum of 20 character at least one number and/or a special symbol .Must be case sensitive. That is, must contain both uppercase and lowercase letters. Passwords are categorized as 'weak', medium' or 'strong'. The user is notified if the password is 'invalid' or 'too short'. The password is classified as 'medium' or 'weak' unless alphabets, numbers and special symbols are used.

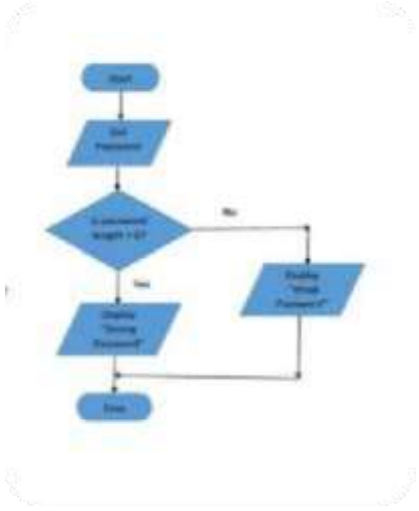


Fig-2 from [2]

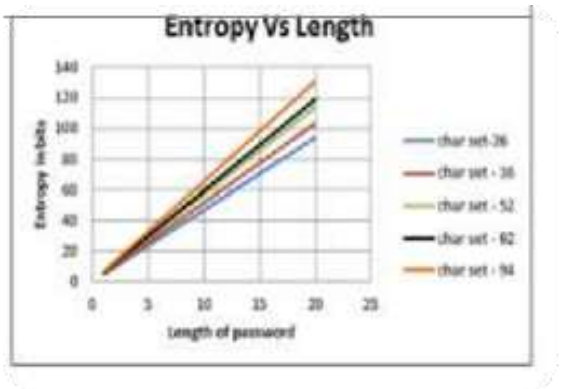


Fig-3 from [2]

4. Results

PAPER	AUTHOR	METHOD	RESULT
[1]	Sivapriya.K, Deepthi.L	Password Segmentation algorithm	In this paper, the authors analyzed three segmentation algorithms namely the Maximum Matching algorithm, Triangular Matrix algorithm, and Password Segmentation algorithm by checking the strength of the passwords and proposed the optimal segmentation algorithm as the best to find a strong password with less or no correlation with user's attributes.
[2]	Yi Yang, AsifKarim, Ronju Ahammad	Password Cracking algorithms, password Entropy	The passwords that were taken as volunteered passwords from the people were tested by the Password Meter a popular online strength-checking website. The Password Meter takes into consideration the character set of the password, the length, consecutive letters, numbers, and repeated characters. They have given the score for those passwords based on which the user can choose a strong password.
[3]	Yimin Guo, Zhenfeng Guo, Yajun Guo	Optiwprds Password Policy - Basic8,3class8,Random8	The authors compared Optiwords with the other three password policies (Basic8, 3class8, and Random8) in a two-part user study with 127 participants. The statistical results showed that Optiwords outperformed the other password policies in balancing security and usability.
[4]	Javier Galbally, Iwen Coisel, and Ignacio Sanchez.	Password Entropy and Correlation	The password is marked on a scale of 10 separately based on the five factors. Then it is averaged, which gives us the result out of 10. If the final score is less than 4, the password is termed WEAK. If the score is equal to or above 8, it is classified as STRONG. Any score in between, the password is termed as FAIR.
[5]	Katha Chanda	Password Strength -Numeric Tests, Alphanumeric Tests, Multi Cases Tests	This Paper providede the various Tests for analyzing the time taken to break the password. On average, almost half of the total number of combinations is tried before striking on the right one. The longer it takes to break a password, the stronger it is. So it is logical to conclude that the greater the length of a password, the better it can stand against a brute-force attack.

5. Discussions

In [1] analysed the password segmentation algorithms and proposed the optimal segmentation algorithm as the best password strength anlyser. In [2] the passwords were tested against the various attacks and the possibilities were tabulated. The password with more number of combinations to crack are termed as strong passwords. In [3] the Optiwords Policy has been compared with other three policies and found that the Optiwords Policy will help a user to keep a strong password. In [4] the chosen passwords were scored out of 10 based on the five factors and the password with high score has been termed as stro ng. In [5] they discussed the entropy of the password and they anlysed the password strength based on the entropy level and correlation of the password with user attributes. This review paper shows that there is still a need to improve the user motive to create a strong password.

6. Conclusion

Password-based verification is that the most generally deployed mechanism to guard user's accounts and private information around the world. Password is a significant key to urge authorization but hackers are much successful in password cracking because of the weak password sel ected by the user. So, the user should select a strong password. The user's selected password's strength should be analyzed. Here, mainly five methods are defined to analyse the strength of the password. From those methodologies, the efficient method that I found is "Password Strengths in terms of Entropy ". As this method analyzes the entropy of the user's selected password, here entropy is used to specify the strength of a password in terms of its information content, measured in bits. A password of m bits strength would need 2m tries to exhaust all possibilities in a brute force attack. Clearly, higher the entropy, greater is the strength of the password. In general the user will get a message which says about the password strength, whether it is strong or not along with this if we display another message which says about the time taken to crack the password then the user may be alerted and will try to have a strong password if it is week. Thus, the password strength analyzer will play an important role in one's security life.

REFERENCES

1. Siva Priya K, and Deepthi L.R, "Password Strength Analyser Using Segmentation Algorithms", 5th International Journal on Communications and Electronics System, 2020.
2. Yi Yang, Asif Karim, "Empirical Study of Password Strength", 5th International Journal on communication and electronics system, 2020.
3. Guo, Yimin, Guo, Zhenfeng; Guo, Yajun (2019). "Optiwords: A New Password Policy for Creating Memorable and Strong Passwords", IEEE Journal of Computers & Security, May 2019.
4. Javier Galbally, Iwen Coisel, Ignacio Sanchez, "A New Multimodal Approach for Password Strength Estimation", IEEE Journal of Information security, Vol.12, No.12, December 2017.
5. Katha Chanda, "Password Security: An Analysis of Password Strengths and Vulnerabilities", International Journal of Computer Network and Information Security, Vol.8, No.7, pp.23-30,2016.
6. Umar Farooq, 2020," Real Time Password Strength Analysis on a Web Application Using Multiple Machine Learning Approaches", INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 09, Issue 12 (December 2020).
7. M, Xu and W, Han, "An Explainable Password Strength Meter Addon via Textual Pattern Recognition". Security and Comm. Networks, 2019.
8. D, Pleacher (n.d.). "Password Entropy". [online] Pleacher.com. Available at: www.pleacher.com/mp/mlessons/algebra/entropy.html [Accessed 28 May 2019].
9. Ebu Yusuf Güven, Ali Boyaci, M.Ali Aydin "A Novel Password Policy Focusing on Altering User Password Selection Habits: A Statistical Analysis on Breached Data". November 2021, Computers & Security 113(5):102560
10. Gongzhu Hu, On Password Strength: A Survey and Analysis.(June 2018)Studies in Computational Intelligence Networking and Parallel/Distributed Computing (pp.165-186)
11. K. Lekshmi ,K.S. Krishnaveni ,V.K. Aparna. "A Hopfield Neural Network Approach for Authentication of Password-Based on Fuzzy Logic".2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI).
12. He, Y., Alem, E.E. & Wang, W. "Hybritus: a password strength checker by ensemble learning from the query feedbacks of websites. Front. "Comput. Sci. 14, 143802 (2020).
13. Rathi Raj, P. Visvanathan, R.Kanchan, Raghav Anand." A Comparative Analysis of Soft computing techniques for Password Strength Classification", 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)."
14. Gelei Deng, Xingjie Yu, Huaqun Guo, "Efficient Password Guessing Based on a Password Segmentation Approach", GLOBECOM 2019 -IEEE Global Communications Conference.
15. Ming Xu, Weili Han, "An Explainable Password Strength Meter Addon via Textual Pattern Recognition" , 2019, Shanghai Key Laboratory of Data Science, Fudan University.
16. M. Golla and M. Dürmuth, "On the accuracy of password strength meters," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, D. Lie, M. Mannan, M. Backes, and X. F. Wang, Eds., pp. 1567–1582, ACM, Toronto, Canada, 2018.