A Reverse Turing test for Estimating Competitive Hardness of Password Recommender System

Abstract: -

Password is the most prevalent and important method to secure user access in majority of online applications, based on what is known prior to the user. There are several online applications such as e-commerce, mail that indicate strength of password set by user. For the first time, we formulate an automated recommender method that generates password based on primary information from user. Also, we analyze the competitive strength of recommender passwords with respect to human users based on the reverse Turing set-up. We propose three classes of hardness denoted by easy, medium, and hard for passwords generated by program. We perform survey that analyzes data on hardness of passwords based on user's choice of hardness for 60 passwords auto generated from 50 user forms. Of these, 20 passwords correspond to easy, medium, and hard classes. Each user has to evaluate 30 passwords for hardness and every password is redundant across 25 different lists. Our experiments indicate the efficacy of password match between program and user based on formulated agreement score. We formulate this gap between user and program assignments, for easy, medium, and hard classes, through information theoretic measures such as entropy of agreement and K-L divergence. The empirical data collected in our survey indicates the Turing separation and Turing closeness of the passwords generated by the machine algorithm that how many users agree with the machine on the strength of the generated passwords and how user-friendly passwords are in regards of usage and remembering them.

Introduction: -

Multi level authentication. Passwords have been a major concern for everyone. The internet has seen massive growth especially in covid era in e-commerce area making it vulnerable to attacks (and create plethora of accounts on various websites), so everybody needs a strong, reliable, and memorable password now and then. But in order to make it more and more memorable people end up making it easy to guess and vulnerable to cyber-attacks. There are many types of cyber-attacks to crack the passwords like a brute-force, dictionary attack, man in the middle and many more. So, the strength of the password becomes a concerning issue.[1] Password strength is commonly understood as a way to measure how difficult it is to break passwords. A common way to enforce the policy is the real-time checking of the password strength during the password selection process by the users. This good practice was already promoted by researchers in the field of password security in the early 1990's.

Although there are many websites available to create or generate a strong password for the users that cannot be cracked easily by the attackers, but it lacks to provide a password that a user can easily use and remember. There has been much research in password generation and password strength estimation and there are various ways used in order to check the strength of a password. The strength of the password is generally estimated by simulating an attack on the password and how the password will stand that attack.

Some of the methods used are: -

Attack Based Approach: - An attack-based approach uses the information about the user and most commonly passwords used by the users to crack the password. It generally uses a brute force methodology. Probably, one of the most direct ways to objectively quantify NoG is to attack a password until it is broken. Most of the works in the state of the art that consider this type of approach are based on a single-attack strategy [1].

Heuristic Based Approach: - It is currently one of the mostly used method to crack a password. It uses a method known as LUDS [counts of lower-case upper-case digits and symbols]. The majority of password policies used in practice are based on this concept [2].

In this paper we will test passwords against multiple approaches and methods used to crack passwords while simultaneously checking its usability with respect to the user as the ultimate goal of a password is that it secures the personal data of a user while being readily usable. The paper will talk about the methodology used in generation and estimation of the password and how it makes sure that it is user-friendly while keeping it difficult for the attacker to crack the password.

References

[1] J. Galbally, I. Coisel and I. Sanchez, "A New Multimodal Approach for Password Strength Estimation—Part I: Theory and Algorithms," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 12, pp. 2829-2844, Dec. 2017, doi: 10.1109/TIFS.2016.2636092.

Abstract

—After more than two decades of research in the field of password strength estimation, one clear conclusion may be drawn: No password strength metric by itself is better than all other metrics for every possible password. Building upon this certainty and also taking advantage of the knowledge gained in the area of information fusion, in the present work we propose a novel multimodal strength metric that combines several imperfect individual metrics to benefit from their strong points in order to overcome many of their weaknesses. The final multimodal metric comprises different modules based both on heuristics and statistics which, after their fusion, succeed to provide in real time a realistic and reliable feedback regarding the “guessability” of passwords. The validation protocol and the test results are presented and discussed in a companion paper.

[2] “Designing password policies for strength and usability,” ACM Trans. on Infor. and Systems Security, vol. 18, pp. 13:1–13:34, 2016.

Abstract

Password-composition policies are the result of service providers becoming increasingly concerned about the security of online accounts. These policies restrict the space of user-created passwords to preclude easily guessed passwords and thus make passwords more difficult for attackers to guess. However, many users struggle to create and recall their passwords under strict password-composition policies, for example, ones that require passwords to have at least eight characters with multiple character classes and a dictionary check. Recent research showed that a promising alternative was to focus policy requirements on password length instead of on complexity. In this work, we examine 15 password policies, many focusing on length requirements. In doing so, we contribute the first thorough examination of policies requiring longer passwords. We conducted two online studies with over 20,000 participants, and collected both usability and password-strength data. Our findings indicate that password strength and password usability are not necessarily inversely correlated: policies that lead to stronger passwords do not always reduce usability. We identify policies that are both more usable and more secure than commonly used policies that emphasize complexity rather than length requirements. We also provide practical recommendations for service providers who want their users to have strong yet usable passwords.

[3] Encouraging users to improve password security and memorability | SpringerLink

Abstract

Security issues in text-based password authentication are rarely caused by technical issues, but rather by the limitations of human memory, and human perceptions together with their consequential responses. This study introduces a new user-friendly guideline approach to password creation, including persuasive messages that motivate and influence users to select more secure and memorable text passwords without overburdening their memory. From a broad understanding of human factors-caused security problems, we offer a reliable solution by encouraging users to create their own formula to compose passwords. A study has been conducted to evaluate the efficiency of the proposed password guidelines. Its results suggest that the password creation methods and persuasive message provided to users convinced them to create cryptographically strong and memorable passwords. Participants were divided into two groups in the study. The participants in the experimental group who were given several password creation methods along with a persuasive message created more secure and memorable passwords than the participants in the control group who were asked to comply with the usual strict password creation rules. The study also suggests that our password creation methods are much more efficient than strict password policy rules. The security and usability evaluation of the proposed password guideline showed that simple improvements such as adding persuasive text to the usual password guidelines consisting of several password restriction rules make significant changes to the strength and memorability of passwords. The proposed password guidelines are a low-cost solution to the problem of improving the security and usability of text-based passwords.

[4] (PDF) PASSWORD SECURITY: WHAT FACTORS INFLUENCE GOOD PASSWORD PRACTICES (researchgate.net)

Abstract

This study will explore variances in password strength across demographics such as age, gender, ethnicity, and education level; organizational password rules; and security training. It also determines the degree to which the individual perception of security threats impacts password strength. By using both personal and employment based accounts, the study will examine whether individuals perceive personal or organizational security as more important. It will also investigate whether the type of account influences password selection. A proposed model for password selection will be described and used to determine if individuals select stronger passwords for accounts with password rules if they understand the risks involved in choosing poor passwords.