Password Checker

Abhishek Kumar Chaudhary[1], Akshay Raj[2], Adarsh Patel[3]
[1,2,3]*School of Computer Science, Galgotias University, GR. Noida, India*

Abstract **- Passwords are 613,584,246 real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they are at much greater risk of being used to take over other accounts. They are searchable online below as well as being downloadable for use in other online systems.**

Index Terms **- Cloudflare, Privacy, Hashing, Encrypting and k-Anonymity.**

I.INTRODUCTION

Passwords are a means by which a user proves that they are authorized to use a computing device. A single device may have multiple users, each with their own password. Passwords are not unlike a lock-and-key system, in which only the right key will enable a person to have access. The difference is that each person has a different key for the same door. Password reuse is normal. It is extremely risky, but it is so common because it is easy and people aren't aware of the potential impact. Attacks such as credential stuffing take advantage of reused credentials by automating login attempts against systems using known emails and password pairs. In today's business landscape, cyber security is often a top priority. Data breaches and other concerns have business owners working hard to find solutions that not only provide the best protection but are also manageable for employees to use.

Unfortunately, in terms of usability, text-based password authentication is quite problematic. A good password needs to be “easy to remember and hard to guess” at the same time, as suggested by Wiedenbeck et al. [59]. However, passwords which are easy to remember are generally short or based on dictionary words (or slight variations). Therefore, these passwords become vulnerable to dictionary attacks. Passwords including personal information are also memorable, but they risk to be guessed by people close to the password owner and attackers that have collected information about the user. Passwords are considered one of the most significant risk factors in terms of security in information systems as they are vulnerable to attacks [8]. This vulnerability is mainly due to user behaviours and practices and not related to the password system itself. The main problem arises from the memorability issue which ultimately causes the other problems related to passwords such as reusing, sharing, and choosing weak passwords.

As described above, human factors play a key role in password security. However, security problems caused by user behaviour have not been totally solved. As previous studies proved that existing password policy rules are not adequate to motivate users to choose strong passwords, this study presents the idea of including several password creation methods in password guidelines and also adding motivating elements to the password creation process without enforcing any restriction rules. Since traditional methods of imposing excessive restrictions have not been very successful, it is suggested that a system that subtly persuades users and offers concrete advice may be more successful. Thus, this study explores whether motivating users with an effective password advice and useful instructions to create strong and memorable passwords is better than obliging users to apply strict password policy rules. This paper recalls the previous studies on password guidelines and reports on an empirical study that has been carried out to evaluate the efficiency of the proposed password guidelines by comparing it with the usual password policy rules.

II.EASE OF USE

Strong Password

One of the concerns that people often have when it comes to creating complex passwords is a fear of forgetting them, particularly when there are several to remember. Naturally, a person should try to think of something that will be easy for them to memorize. One way to do that is to turn a sentence or phrase into something that is not easily recognized by others. To

do this, use the first letter of every word in the sentence, replacing certain words with numbers or symbols. For example, the word "for" may be replaced with the number 4 or the word "number" with the # symbol. With this method, a password such as "Save the number for later in the year" may read St#4LITY.

III. EXPLANATAION

Authentication is one of the most important areas in computer security, and the use of traditional text-based passwords has been well studied. However, this type of authentication mechanism has drawbacks. Various alternative authentication schemes which aim at aligning security and usability have been proposed. These proposals range from graphical password authentication to location-based authentication [22,26,53]. However, none of these schemes could overcome the simplicity and affordability of typing a sequence of keyboard characters to allow authenticating users. As a result, traditional text-based passwords are still the most popular Before you begin to format your paper, first write, and save the content as a separate text file. authentication mechanism on the Web, and they are likely to remain so in the near future. Unfortunately, in terms of usability, text-based password authentication is quite problematic. A good password needs to be “easy to remember and hard to guess” at the same time, as suggested by Wiedenbeck et al. However, passwords which are easy to remember are generally short or based on dictionary words (or slight variations). Therefore, these passwords become vulnerable to dictionary attacks. Passwords including personal information are also memorable, but they risk to be guessed by people close to the password owner and attackers that have collected information about the user. Passwords are considered one of the most significant risk factors in terms of security in information systems as they are vulnerable to attacks. This vulnerability is mainly due to user behaviours and practices and not related to the password system itself. The main problem arises from the memorability issue which ultimately causes the other problems related to passwords such as reusing, sharing, and choosing weak passwords Complete all content and organizational editing before formatting.

A. Background and Related Work

DTo increase the strength of user-chosen passwords, users are typically required to adhere to a set of rules known as password guidelines when creating passwords. Users compose their passwords following the specific requirements given in the guidelines. For example, the password must contain at least eight characters including at least one number or one upper case letter, and it should not contain the username. There are various password guidelines that are used by organisations, and they should be written efficiently to provide adequate security levels in the organisations [7,52].

According to a study, a user has on average 25 online password-required accounts and uses eight passwords per day [19]. However, nowadays, users may even have much more than 25 passwords. As users are expected to use different passwords for each account to avoid security failures, it is difficult for the brain to remember many discrete sets of illogical and random bits of information and then associate each set with which account. The user’s response to this situation is generally adopting strategies such as choosing weak passwords or writing them down, which ultimately undermine the security of the systems they use [36]. Some methods are used to replace this subversive behaviour with appropriately suitable behaviour for authentication [60]. These methods aim to direct user behaviour by implementing strict password creation guidelines, proactive password checkers or password expiry, to ensure a high security level. In addition to these, password management systems are also used nowadays. To save many passwords in a system may be a solution for the memorability problem, but it is also problematic regarding security since the protection of all passwords depends on one single password named “master password”. If the master password is cracked, then all user’s passwords are obtained. Recent research shows that these advice, measures, or system features do not always work as expected. They sometimes have negative effects upon usability and security, contrary to designers’ intentions. Where users are given unreasonable constraints, they may more likely adopt insecure workarounds which are easy to use for them [47]. As it is well known, users mostly do not follow the strict security guidelines prescribed within authentication schemes. sed in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

B. Password Creation Policies

- Password restriction policies are a series of rules which determine the content and format of the passwords accepted by an authentication system. These policies are used by system administrators to enhance computer security by guiding users to create more secure passwords.
- In 2006, the National Institute of Standards and Technology (NIST) updated the "Electronic Authentication Guideline" [6] to be used by security system administrators for the implementation of electronic authentication.
- They found that users have less difficulty to comply with creating a 16- character minimum password compared to an 8-character minimum excluding dictionary words or further restrictions. In addition, passwords with at least 16-characters provide the best security".
- Identify applicable funding agency here. If none, delete this text box.
- Contrary to what is believed, some researchers have claimed that password restriction policies do not improve password security.

Password Creation Advice

Most systems that impose password restrictions offer their users password advice about creating passwords. The purpose of password advice makes adoption of password policy rules easier and also motivate users to create stronger passwords. In a study, password practices of ten popular Internet sites which enforce password policy rules and offer password advice were examined [23]. That the websites' password restriction policies and password advice are vastly different, sometimes caused conflict between them. In most of the websites, password advice was found ambiguous and unhelpful by users. As existing password policies and advice are far from being consistent and effective, it is not easy for users to form accurate mental models of how to create a secure and memorable password.

Mnemonic Passwords

There is a wealth of research investigating the best way to advise users to create secure and memorable passwords. In an attempt to encourage users to create easy-to remember passwords, mnemonic phrase-based passwords have been first proposed by Barton and Barton [2]. Mnemonic passwords are derived from a memorable sentence where users generally use a letter of each word in the sentence. Although most of the password advice research is about mnemonic passwords, they are rarely recommended to use in practice [23]. There are more studies which present the different ways to generate a mnemonic password. Vu et al. [57] used two mnemonic password generation methods in a user study, and let all users choose their own sentence. As the passwords created with the mnemonic string method typically have more characters, they were thought more secure. However, the authors found little difference in password creation times, login times and recall error rates between two methods. In a previous study, they had also found that passwords which contain more characters were more resistant to cracking [47]. Unfortunately, as the way of substitute words and characters suggested in the study is well known by attackers, mnemonic string method may not be very much secure as previously thought.

Memorability

Memorability is the most important issue in knowledge-based authentication systems considering the limitation of human memory that puts systems security into high risk. Many studies pointed out the users' difficulty in remembering passwords [1]. Users typically adopt coping strategies to avoid forgetting and resetting passwords. Vu et al. [57] tested the memorability of text passwords which are created obeying various password policy rules. They found that remembering five passwords is more difficult than remembering three passwords. Also, users tend to create passwords which are obviously connected to the accounts, as a memory assistance coping strategy. Chiasson et al. [12] conducted a study to compare the memorability of multiple text passwords and multiple PassPoints graphical passwords (a PassPoints password is a sequence of points, chosen by a user, on an image). They found that after the passwords were created, graphical passwords were much more easily remembered than text passwords. As remembering different passwords across accounts is challenging for users, they commonly use coping strategies to overcome the memorability issue. One of these strategies is choosing similar passwords across accounts which causes multiple password interference. This issue has been studied in a few other graphical passwords-related research papers [11,18,42].

Password creation advice

Most systems that impose password restrictions offer their users password advice about creating passwords. The purpose of password advice makes adoption of password policy rules easier and also motivate users to create stronger passwords. In a study, password practices of ten popular Internet sites which enforce password policy rules and offer password advice were examined [23]. That the websites' password restriction policies and password advice are vastly different, sometimes caused conflict between them. In most of the websites, password advice was found ambiguous and unhelpful by users. As existing password policies and advice are far from being consistent and effective, it is not easy for users to form accurate mental models of how to create a secure and memorable password. Murray and Malone [43] recently highlighted the characteristics of the password advice distributed by different organizations. They found out that there are substantial discrepancies between advice used in different environments. Websites enforce different password creation restrictions.

Their research also showed that some advice stated as the best practice by security researchers is even not included in the majority of advice. This contradiction may cause users unwillingness to follow advice. There are more studies which present the different ways to generate a mnemonic password. Vu et al. [57] used two mnemonic password generation methods in a user study, and let all users choose their own sentence. As the passwords created with the mnemonic string method typically have more characters, they were thought more secure. However, the authors found little difference in password creation times, login times and recall error rates between two methods. In a previous study, they had also found that passwords which contain more characters were more resistant to cracking [47]. Unfortunately, as the way of substitute words and characters suggested in the study is well known by attackers, mnemonic string method may not be very much secure as previously thought.

Password advice can also be represented with a tool measuring strength of the password and giving users a numerical result or statements such as 'weak', 'strong' and 'very strong'. These tools are called "password strength meters" which typically illustrate the strength of the currently chosen password when a user is registering for an account. The meters are commonly used by popular websites (Gmail, PayPal, and eBay). In an online user study conducted with over 2000 participants, different password strength meters were evaluated [55]. The results showed that the passwords created by users who used password meter were more difficult to guess than the passwords created by users who did not use a strength meter. Furthermore, users created much stronger passwords when they used stringent password meters. However, the authors found that meters which are too stringent may cause users to lose motivation and ignore the meter. In another study, a novel method called adaptive password strength meters (APSMs) were proposed to measure password strength [10]. Adaptive password strength meters use Markov models [40] to measure a password's strength as the collective probability of each character following the previous characters in the password. These probabilities can be calculated based on either a training set of passwords or the passwords currently in use. Although the authors claim that APSMs are better than any other proposed password strength metric to date as it can score passwords closer to the "ideal" password strength meter, there has not been conducted any formal usability study of APSMs and a practical security evaluation. Kelley et al. [35] introduced different calculators for estimating the number of guesses required to crack a password using a particular cracking algorithm. They calculated the percentage of passwords which can be cracked with the implemented algorithm given a number of guesses. To compare cracking performance across algorithms, guess number calculators for several cracking algorithms on the same set of passwords can be implemented. Guess number calculators may be considered the more practical and efficient method of proactive password checking [3] than running a computationally intensive password cracking algorithm.

IV.CONCLUSION AND FURTHER RESEARCH

Although the use of passwords as an authentication method has been extensively studied in the past, there are no empirical studies that test the effectiveness of password creation methods. Thus, the contribution of this research and its implications for both research and practice are significant. As the results of the empirical studies indicated, the proposed password guideline improves the security and memorability of user-chosen passwords. Rather than obliging users to

follow strict password policy rules, motivating, and directing them to create strong and memorable passwords seems more efficient and usable way. Thus far, the results generally have shown some promising findings; however, the practicability of this new password guideline may be an issue in real world, as stated above. The password guideline can be improved adding visual elements in the guideline to make reading the given information process interesting. It would probably be useful to attract users' attention and make the password creation process more enjoyable. Also, implementing the proposed password guideline into different kinds of applications which require different levels of security and conducting a further empirical study with different user groups involving more participants would be useful. Also, giving users some feedback during the password selection process such as meter-based ratings would motivate users to choose more secure passwords. Moreover, the literature on persuasion suggests that persuasion attempts are more likely to succeed if the persons are aware of the situation. Thus, adding some attributes to the password guideline informing users about possible attacks if they choose weak passwords might improve the compliance to password guideline.

REFERENCES

[1] Adams, A., Sasse, M.A.: Users are not the enemy. Commun. ACM42(12), 40–46 (1999). https://doi.org/10.1145/322796.322806

[2] Barton, B.F., Barton, M.S.: User-friendly password methods for computer-mediated information systems. Comput. Secur. 3(3), 186–195 (1984)

[3] Bishop, M., Klein, D.V.: Improving system security via proactive password checking. Comput. Secur. 14(3), 233–249 (1995)

[4] Bonneau, J., Herley, C., van Oorschot, P.C., Stajano, F.: The quest to replace passwords: a framework for comparative evaluation of web authentication schemes. In: Security & Privacy (SP), IEEE Symposium, pp. 553–567 (2012)

[5] Burnett, M., Kleiman, D. (eds.): Perfect Passwords. Syngress Publishing, Inc, Massachusetts (2006)

[6] Burr, W., Dodson, D., Polk, W.: Electronic Authentication Guideline. Special Publication 800-63 Version 1.0.2. National Institute of Standards and Technology (NIST), Gaithersburg (2006)

[7] Campbell, J., Ma, W., Kleeman, D.: Password composition policy: does enforcement lead to better password choices.