Convenience or Strength? Aiding Optimal Strategies in Password Generation

Michael Stainbrook[1], Nicholas Caporusso[1]

[1] Fort Hays State University, 600 Park Street, Hays, United States
{mjstainbrook, n_caporusso}@mail.fhsu.edu.com

Abstract. Passwords are a wide-spread authentication method used almost unanimously. Though the topic of passwords security may seem old, it is more relevant than ever. This study examines current user-password interactions and classifies them in terms of convenience and security. Findings show that users are aware of what constitutes a secure password but may forgo these security measures in terms of more convenient passwords, largely depending on account type. Additionally, responses show that users are very motivated to reuse or create similar passwords, making them easy to remember and including something meaningful to them. Finally, researchers provide discussion of the results along with a conclusion and recommendations.

Keywords: Security · Convenience · Password Management · Cybersecurity

1 Introduction

Passwords are a widespread authentication method that almost all users utilize when signing into their accounts. Although several devices implement alternative identification mechanisms, alphanumeric text is still the most utilized authentication system. Nevertheless, ranging from local host accounts, to email and social media, users must create or reuse passwords for an average of 25 different accounts [1]. Thus, when creating passwords for new accounts, users may implement different password creation strategies. Specifically, the main component is the trade-off between security and convenience, with the latter involving a shorter password consisting of dictionary words or text which is easy to type or remember. Indeed, as entropy increases with length and complexity, convenience usually is negatively correlated with security. Moreover, as users must memorize multiple passwords, they may forgo creating secure passwords to create more convenient and easier to remember codes.

In this paper, we analyze the human factors behind passwords creation strategies and users' awareness in terms of security of both authentication system (i.e., type of authentication, strength of the keycode, and time to crack) and context of use (e.g., computer login, website, Wi-Fi network, and social media). Specifically, we investigate the underlying motivations in the approach to trade-offs between security and convenience in password generation. To this end, we discuss the preliminary results of an experimental study in which we analyze data from 100+ users. Our objective is to identify clusters within the wide range of password creation strategies, with users' decisions falling into

categories of security and convenience depending on specific factors that can be incorporated in a predictive model. Then, we use the data to implement and train a simple classifier that can be utilized to evaluate and support password decisions in terms of convenience and security. Furthermore, consistently with the literature, our results show that account type is the biggest identifier for users creating passwords.

As discussed in several studies, most of the users already are aware of how to create secure passwords [2]. Nevertheless, our findings show that they may still deliberately aim for an easier to remember albeit less secure code. Therefore, we detail how security can be enforced without compromising convenience by introducing a system that provides individuals with real-time information about the strength of the password they are generating, using standard measurements for password security (i.e., entropy, time to crack) and context information. Moreover, by analyzing the complexity and structure of the password, our system can suggest improvements to both convenience and security within the same trade-off cluster. Alternatively, the system can provide users with recommendations on how to get to nearby clusters (i.e., enforce security or increase convenience) with minimal effort. To this end, several stop criteria can be set so that more convenient and secure passwords can be achieved by replacing, adding, or even removing a single character. As a result, by addressing human aspects, the system can assist users with optimal strategies for password generation.

2 Related work

The first passwords were created in the 1960s and allowed users to access MIT's time-shared computer mainframes. Improved security was the reason passwords were first implemented as students began playing jokes and pranks after obtaining other users passwords through guessing or gaining access to the master password file. Ultimately, passwords were created to verify that a user was who they said they were while interacting with the mainframe. Throughout the years, passwords became more secure with the introduction of cryptography and secure sockets layer (SSL). Passwords quickly evolved and in the 1990s expanded to include certificates at the SSL layer, allowing users to authenticate their identity to the server. These passwords were text-based and incorporated into systems such as e-commerce and internet accounts [3].

Current user password practices can be summarized as: creating insecure passwords, reusing and forgetting them. Although research has shown that users are aware of what a secure password consists of [2], other studies [1] found that users typically choose weak passwords with a bit strength average of 40.54 and mostly lowercase letters. Thus, users tend to forgo creating secure passwords, possibly due to the password paradox, stating: average users need to create secure, strong passwords, and not write them down. Moreover, these passwords need to be strong enough that no user will remember them. Therefore, users may forgo creating secure passwords as they are not easy to remember and inconvenient. A study of agent based human password model found that the more often a password is forgotten, the higher chance that it will subsequently be written down, a possible security breach. Therefore, the easier it is for a password to be reused or remembered, the less likely it is to be written down [4]. Thus, users tend to forgo creating secure passwords in favor of an easier to remember, less secure password.

A study about users' perceptions during password creation [5] found that providing users with real-time feedback and requirements (in a three-step process) can increase usability and security, and reduce errors in recalling the password; however, the resulting passwords showed less security than expected in terms of time to crack: passwords created with real-time feedback had 21.7% chance of being of cracked in $2x10^{13}$ attempts, and adding short random text dramatically increased password strength [5].Furthermore, as users are having to manage many accounts, they may be opting to use sign in options that might compromise security with improved convenience, such as, Single sign-on (SSO), which is an authentication method that enables users to sign in to a site or service using a separate account, such as, social media (e.g., Facebook, Twitter, or Google+), minimizing the number of passwords users need to remember. Although SSO adds security compromise, 41.8% of respondents reported they would continue using SSO after learning about their vulnerabilities [6].

Several studies found that users are aware of what a secure password consists of along with convenience being a major factor in password selection along with the type of account the password is for [2]: examples of secure passwords consisted of combinations of at least eight letters and number characters, whereas bad password include names and relevant personal information, such as, birthdate and phone number. Additionally, security and convenience have a direct negative correlation, and both dimensions depend on the account type: more secure passwords are more likely to be utilized in creating an online banking account than in a secondary email account. Moreover, time-frame also has a factor in the influence of password creation: users who are given not enough time or too much time to create passwords choose less secure passwords [2].

3 Study

As passwords are an established measure, the topic has been studied extensively. However, in today's digital society, users have more accounts than ever [1]. New and convenient methods such as Single Sign-on [6] might help users relying on a few passwords and consequently increasing their security. However, the purpose of this study was to examine the human factors of password creation to improve password generation techniques by designing and implementing new user-centered tools that take into consideration users' individual behavior in improving the convenience and security trade-off.

We created a digital survey, which was published on social media along with researchers gathering participants from Fort Hays State University via classrooms, colleagues, and word of mouth. The questionnaire was designed to capture the following elements:

- how many passwords they remember and use
- how often they typically change their passwords
- what type(s) of password management system they use
- if any of their accounts have been hacked before
- when creating new passwords how motivated they are to include certain aspects
- how often they forget their passwords
- how likely they are to include different aspects and characters in their new passwords

- the main reason why they change their passwords
- how secure they believe they make their passwords for different accounts types
- main concerns with potential risks for their passwords.

Participants were recruited for the study via university classes, colleagues, word of mouth, e-mail, and researchers posting the survey link on social media. Demographic information gathered included age, education level, and primary education background.

A total of 114 responses were gathered from the study with (34.2%) in the 18-24 age range, (28.1%) in the 25-34 group, (28.9%) in the 35-54 group, (7.9%) 55+, and (.9%) prefer not to answer. The educational level achieved by participants was: bachelor's degree (32.5%), high school graduate (23.7%), master's degree (23%), doctorate degree (11.4%), associate degree (7.9%), and other (1.8%). Primary educational background information of participants was informatics (21.9%), business (13.2%), education (11.4%), engineering (10.5%), communication (8.8%), science/social sciences (5.3%), psychology (5.3%), and other various education backgrounds ranging from theatre, virology, tourism, graphic design, ministry, and other (23.6%). Results were collected and then analyzed on factors, such as, demographic information, password security and convenience, and user concerns for their accounts.

4 Results and discussion

Our data show that the majority of users are actively using between 3 and 6 passwords per day (Fig. 1, left). Age has a significant role in the number of passwords, as users who are 35-54 reported using the largest number of unique passwords (4-10), as shown in Fig. 1 (right). This might be due to larger familiarity with and use of SSO of users in the other age groups.

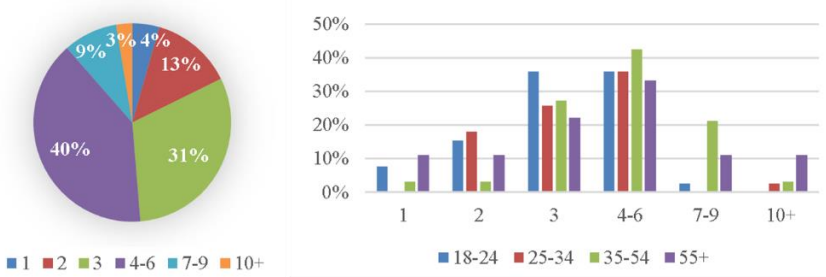

Fig. 1. Unique passwords used per day (left). Users reported 3-6 passwords a day (70.2%), 2 passwords (13.2%) and 7-9 passwords (8.8%). Percentages of unique passwords used per day categorized by age group (right). Sixty-six percent of the 35-54 age group reported using from 4-10+ passwords every day (66.6%).

A large group of respondents (48.2%) reported that their password update frequency depends on the website or account, 21.1% indicated changing their passwords every 3-6 months, and 12.3% reported they never change their passwords. Furthermore, it appears that many users are not using a password management system other than their memory (Fig. 2).

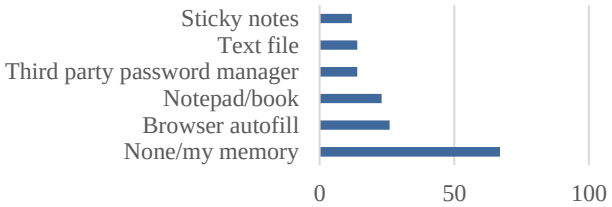

Fig. 2. Password management system(s) used with the x-axis representing number of users. The majority of users reported only using their memory to manage passwords (58.8%).

When questioned about password creation behaviors, almost 70 percent of respondents answered motivated or higher to create passwords similar to others they use (69.2%). In addition, users reported motivated or higher to include something meaningful to them in their password (57%), and to consider the security of the password during creation (58.8%). Contrastingly, when questioned about level of motivation to create a password that a family member/friend could use as well, seventy-seven percent reported unmotivated to very unmotivated (77%), with a little over half also responding unmotivated or very unmotivated to write their password down in a password manager or system (51.8%). When asked how often they forget their passwords, most users indicated rarely (41.2%) or sometimes (39.5%). Furthermore, when comparing users who reported using a password manager to users who reported not using a password manager, it appears that some groups of users indicated forgetting their passwords regardless of the system used (see Fig. 3). All communications background respondents reported forgetting their passwords often even while using a password management system.

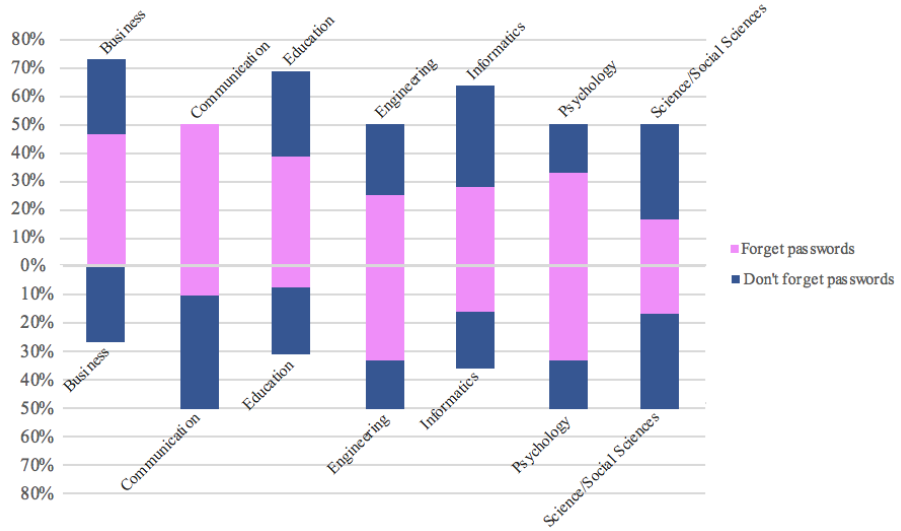

Fig. 3. The percentage of users who indicated remembering or forgetting passwords while using a password management system. The top percentage represents users who reported actively using

a password manager and the bottom percent represents users who reported not using a password manager of any kind.

The majority of participants (71.1%) reported that they are very likely to make their passwords easy to remember and similar to other passwords they use (70.2%) and to include something meaningful to them (60.1%). Furthermore, when questioned about the likelihood of including different characters in their passwords, users were likely or very likely to include numbers (89.5%), special characters (70.2%), upper-case letters (78.1%), and to include more than 8 characters (78.9%).

The main reason for changing passwords is forgetting them, with the second being the account management forcing them to (Figure 4).

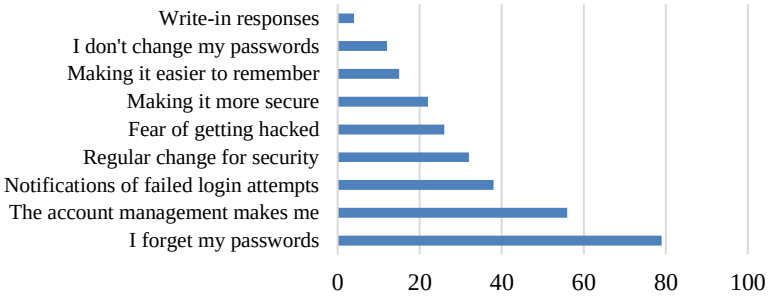

Fig. 4. The main reason(s) users change passwords with the x-axis representing number of respondents. Changing due to forgetting and resetting them (69.3%), account management makes them (49.1%), and notifications of failed login attempts (33.3%).

Participants were also asked about their main concerns with the potential risks for their accounts and passwords. Respondents were most concerned with identity theft and privacy issues (see Fig. 5)

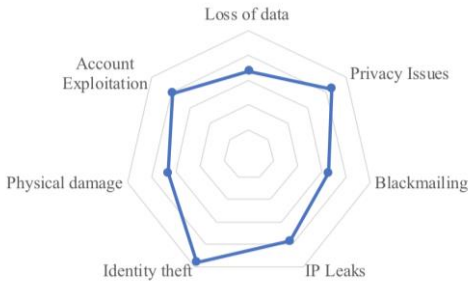

Fig. 5. Users levels of concern for their accounts. Respondents indicated being mid to most concerned with identity theft (96.5%), privacy issues (85.1%), account exploitation (78.9%), IP leaks (77.2%), loss of data (76.3%), physical damage (66.6%), and blackmailing (65.8%).

When questioned about their passwords for different account types in terms of security and convenience, users reported making certain accounts such as social media (65.8%) and Bank accounts (88.3%) to be secure or very secure. Contrastingly, some

users were willing to give up security in favor of convenience for certain accounts, such as personal and work computer sign-ins indicating making their password neutral to very convenient (46.5%) and (50%) respectively.

Moreover, data was also analyzed by educational background. When comparing educational background for creating similar or reusing passwords, many were motivated or very motivated to do so (see Fig. 6).

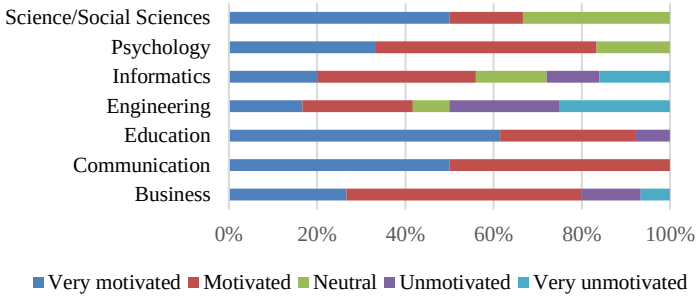

Fig. 6. Percentages of user levels of motivations in creating or reusing similar passwords by educational background. Many were motivated or very motivated, communication (100%), education (92.3%), psychology (83.3%), and business (80%).

When questioned about participants level of motivation for considering the security of their passwords, informatics, business and engineering users responded the highest percentage of motivated or very motivated at (64%), (73%), and (83.3%) respectively. Furthermore, when questioned about the likelihood of creating passwords that are easy to remember, many users were motivated or very motivated to do so. When considering all users being likely or very likely to create easy to remember passwords, psychology and science/social sciences were (100%), communication (90%), and business (86%).

Moreover, when analyzing user averages in likeliness to include positive password security factors, users were very likely to use numbers, upper-case letters, and to include more than 8 characters. Users were very unmotivated to check the entropy or include a random string of characters (Fig. 13 left).

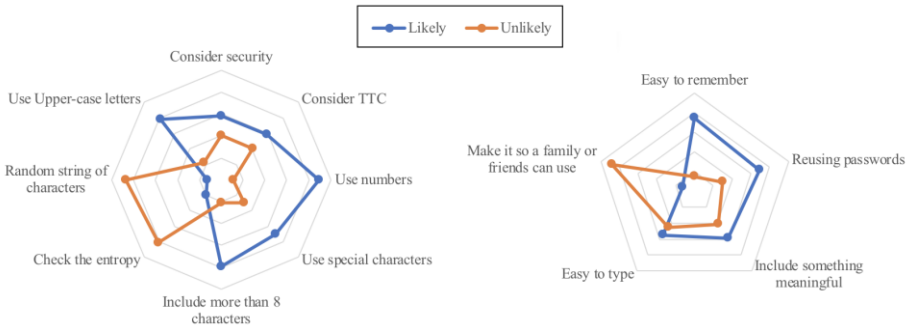

Fig. 7. User averages of likelihood to include positive security factors in their passwords (left). User averages of likelihood to include convenience factors in their password (right).

Additionally, when analyzing user averages in likeliness to include convenience factors, users were more likely to make their passwords easy to remember, reuse passwords, include something meaningful, and make them easy to type. Users were unlikely to make passwords so a friend or family member can use them and a small group was unlikely to make their passwords easy to type (Fig. 7 right).

Our findings show that users are motivated to include different convenience factors in their passwords. Users were very motivated to create passwords that are easy to remember, similar or reused. Also, participants include items that are meaningful to them, which, in turn, might be detrimental in terms of security, because it might involve the presence of dictionary words and information, such as, birth date, that can be discovered. Creating passwords in this manner most likely correlates to that finding that over half of respondents reported only using their memory to manage their passwords. Interestingly, users indicated that it depends on the website or account for how often they change their passwords; however, users overwhelmingly reported the main reasons they change their passwords is from forgetting the password, the account management makes them, or notifications of failed login attempts. Thus, users are not motivated to change their passwords unless forced to do so. Moreover, this may support the password paradox [4], in that users may not be creating secure passwords as they are difficult to remember, and many users reported only using their memory to manage passwords.

Additionally, our findings agreed with [2], in that account type is the largest identifier for the security of passwords. Eighty-eight percent (88.3%) of respondents reported making their bank account passwords secure or very secure; whereas, with personal computer sign-ins some users were more likely to give up security for a more convenient password. Additionally, our findings suggest users from communication, education, psychology and business backgrounds may need more security training. Users from these backgrounds were extremely likely to reuse passwords and less likely to consider the security of new passwords. Furthermore, as a majority of users only use from 3 to 6 passwords, it may be in their best interests to find a mix of convenience and security that best suits the user.

There are several strategies that can be utilized to help users create 3-4 convenient easy to remember passwords. Considering the attitude towards password creation, real-time feedback in the password generation process might lead to significantly improving password security. Several systems force users to adopt security standards, such as, having at least a specified length, including special characters. However, as previous studies found [4], when security items are specified as a list of requirements, users will stop improving the strength of their password as soon as they meet the bare minimum set suggested by the guidelines. Therefore, our research suggests that one of the potential directions for improving real-time feedback during password creation could be adding mechanisms to raise individuals' awareness about security metrics, such as, entropy and time to crack: showing the expected time for guessing the chosen password might help users identify vulnerabilities in their current selection and, in general, in their password creation strategy.

Moreover, real-time password feedback could provide users with suggestions on small changes to their passwords that would add security factors. For instance, including elements, such as, special characters, numbers, random strings, and uppercase and lowercase variation. Thus, users could evaluate in real-time the security increase while

they are creating their passwords, and choose the best combination that would not compromise convenience or that would result in the best convenience and security trade-off. By doing this, password generation aiding tools would inherently embed a simple security training in the process: users would learn how to improve security by tweaking their password and using the response of the system as feedback to evaluate how different characters impact security. Moreover, they could define a satisfactory convenience level based on the time to crack instead of the "checklist" approach offered by current systems using requirements lists.

In addition, password aiding tools could take into consideration the hosting service and the security measures it implements, to suggest a password entropy target that would improve time to crack and add to the vulnerability mitigation strategies that are already in place. Also, systems that have access to more detailed users' demographics might provide suggestions based on the different educational backgrounds and cope with profiles which reportedly use unsecure password practices.

Also, as many users reported only changing their passwords when they forget them, aiding tools could suggest creating passwords for accounts used irregularly to be very secure, as users will most likely forget the password and reset them regardless. As a result, this would help users create 3-4 convenient, easy to remember passwords, then tweak these passwords to include positive security factors such as different characters and adding length. Users should actively create a secure password management system and educate themselves regularly about improving password security to receive the most security from their passwords to protect their private data. Finally, tools for improving password security strategies should involve the authentication phase, in addition to account creation: reminding users of the time to crack of their password, how it decreases with technology advances, and showing them elements, such as, the time since the last password change, could improve users' awareness and motivation to change passwords more regularly.

5 Conclusion

Although passwords have extensively been studied in several decades of cybersecurity literature, their importance grows with the number of accounts and with the increase in processing power which, in turn, reduces the time to crack. Moreover, the introduction of new and convenient authentication methods, such as, Single-sign on, minimizes the efforts in managing multiple passwords, though it might compromise security. Furthermore, users will most likely not be able to use convenient sign-in methods for bank accounts, government websites, or educational services. Therefore, the security and management of users' passwords will be significant for accessing and securing users' digital resources through future online accounts.

The present study is part of a larger body of research aimed at designing tools for helping users achieve the best security and convenience trade-off by suggesting them how to improve their password in real-time, when they are creating their account or when they are renewing their password. To this end, we focused on the human factors of password creation and how they influence the convenience and security trade-off to better tailor the design of our system to users' needs and practices, and to serve them better with password generation aiding tools that blend in with users' behavior. Our

findings suggest that users are aware of how to create secure passwords; however, they may give up some security factors in favor of a similar and easier to remember password that includes something meaningful to them. This research has several limitations, including missing information about users' actual passwords, which would have added some validation criteria to the analysis of the results of the questionnaire. Indeed, we did not want to acquire and analyze users' passwords, because some of the respondents could not feel confident in participating to the study and because password security will be the focus of a follow-up study, in which we will disclose the design of the system.

Nevertheless, our findings show that human factors, and specifically, the tendency to create easy to remember password with a personal significance has a significant role in the compromise between security and convenience, with users having a slight preference for the latter. This is demonstrated by the limited number of different passwords, by the limited use of password management systems, and by the password update frequency.

References

1. Florencio, D., and Herley, C. (2007). A large-scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web*, 657–666. ACM.
2. Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: A tradeoff between security and convenience. *Behaviour & Information Technology, 29*(3), 233-244. doi: http://dx.doi.org/10.1080/01449290903121386
3. Bonneau, J., Herley, C., Van Oorschoto, P. C., & Stajano, F. (2015). Passwords and the evolution of imperfect authentication. *Communications of the ACM, 58*(7), 78-87. doi:10.1145/2699390
4. Korbar, B., Blythe, J., Koppel, R., Kothari, V., & Smith, S. (2016). Validating an agent-based model of human password behavior. In *The Workshops of the Thirtieth AAAI Conference on Artificial Intelligence*, 167-174.
5. Shay, R., Bauer, L., Christin, N., Cranor, L. F., Forget, A., Komanduri, S., ... & Ur, B. (2015, April). A spoonful of sugar?: The impact of guidance and feedback on password-creation behavior. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 2903-2912). ACM.
6. Scott, C., Wynne, D., & Boonthum-Denecke, C. (2017). Examining the privacy of login credentials using web-based single sign-on – are we giving up security and privacy for convenience? Symposium conducted at the IEEE Cybersecurity Symposium (CYBERSEC), 2016, Coeur d'Alene, Idaho. doi: 10.1109/CYBERSEC.2016.019