A SURVEY STUDY OF PASSWORD SETTING AND REUSE

by

Qi Li

A thesis submitted to the Faculty of the University of Delaware in partial fulfillment of the requirements for the degree of Master of Science in Electrical and Computer Engineering

Summer 2020

A SURVEY STUDY OF PASSWORD SETTING AND REUSE

by

Qi Li

Approved: _____
Haining Wang, Ph.D.
Professor in charge of thesis on behalf of the Advisory Committee

Approved: _____
Mark S. Mirotznik, Ph.D.
Interim Chair of the Department of Electrical and Computer Engineering

Approved: _____
Levi T. Thompson, Ph.D.
Dean of the College of Engineering

Approved: _____
Douglas J. Doren, Ph.D.
Interim Vice Provost for Graduate and Professional Education and
Dean of the Graduate College

ACKNOWLEDGMENTS

I would like to express my special thanks to Professor Haining Wang for his patience, encouragement, and immense knowledge. His advice helped me in all the time of conducting this research.

I would also like to thank all the participants of the survey. Their patience and careful responses are the key to completing this research.

TABLE OF CONTENTS

LIST OF TABLES

ABSTRACT

Password security is strongly tied to a user's password setting and reuse. The purpose of this thesis research is to explore the current status of users' password usage, and to explore possible resolutions to enhance password security based on users' password behaviors. A survey was conducted to provide data for this research. There are 10 questions included in the survey, which covers the topics of password setting behaviors, password fatigue, and password reuse. We collected 175 answers in total from all participants and selected valid answers and analyzed them. Based on the results, we can see that the current users' password behaviors are not optimistic because of the negative influence of password fatigue and a lack of knowledge about the secure password management strategies. This thesis suggests people should acquire more knowledge related to password security, or even information security, during school education. And the service providers and developers should take the responsibility of protecting users' passwords not only by enhancing the security structure of their products, but also by providing users more advice and instructions about the feasible ways to increase password security.

Chapter 1

INTRODUCTION

Why Password Security Matters

People are having an increasing number of accounts that require passwords for authentication during the login process. As passwords become more frequently used in our daily life. The risks associated with passwords have become noticeable. According to the research by Pearman, Thomas and Naeini [1], improper password setting habits and multiple usage of the same password for different accounts are common causes of account security risks.

It is a natural tendency that people prefer a simple way when log in to their accounts. However, the login process for websites that require multiple authentication procedures seems to make the process more complex. For instance, besides account password, some websites also require security questions or CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart). Therefore, users may choose to simplify their password to make the login process easier as CAPTCHA is mandatory [2]. However, the easier the passwords are generated, the higher the security risks are. Moreover, the experience of password fatigue makes users change passwords less frequently, which also increases the security risk.

Based on the related paper and personal review, the most common problem in our daily life is the improper password creation, and then multiple usage of the same password in different websites. The easier way we create our password, the higher decryption risk

we could get. And repeated use of the same password on different websites could bring us high security risk of being broken down all the accounts.

The purpose of this paper is to investigate the current situation of preference of people generating password, the fact of password fatigue and password reuse. And to find the logical connections between people's password habits and the security issue. I hope this research could arouse people's awareness of their password security.

Chapter 2

BACKGROUND

The Fact of Text-based Password and What is Urgent

The types of password vary. This paper will particularly focus on the security topics of text-based password. Text-based password, as a form of most common type of password, is frequently used for log-in authentication of online accounts. Text-based passwords are widely criticized for its potential security risk and are broadly used by our Internet services and computer systems for user authentication in current times due to its ease of use. At the same time, it is also vulnerable [3]. Memory lapse, possibility to be stolen or cracked, password reuse, are all factors that discredit the safety of text-based password. Nonetheless, text-based password is still a common and widely used type of password. Other types of password, such as graphical password, voice password, and fingerprint, have their advantages in convenience and security. However, due to the hardware constraints, those types have not been widely adopted by services providers. It is unlikely for text-based passwords to be replaced in the short period of time. Therefore, the security concerns of text-based password will still be a focal topic of account security.

Nowadays, there are so many different types of websites online such as social media, online shopping, financial support and even tax return. They all need us to create new accounts and set different passwords with some specific requirements to ensure account safety. This kind of situation caused two phenomena. First, people tend to set their passwords closely related to their personal information so that it will not be easily forgotten. Second, too many similar new passwords setting experiences would make people suffer

password fatigue and then prefer to use several fixed passwords for all their accounts in tangled websites. However, this behavior will lead to improper password setting and reuse. It would highly lower the account security and largely increased the risk of our multiple accounts being hacked and broken down at the same time.

Beside enhancing the data security for service providers, it is also important for users to understand the proper and secure ways to manage their passwords. It is plausible that password habit has a strong connection to users' account security [4]. Bad password setting habits, such as oversimplification, password reuse, or using personal related information in the password generating process, makes users' passwords vulnerable. The study of password security should pay attention to users' password using habits and understand the reasons behind the habits in order to provide more feasible and pertinent resolutions. Therefore, in this paper, a survey related to password setting and reuse has been conducted to find out the habitual way of people setting passwords, the general situation of password fatigue and reused password usage cases for multiple accounts. It will help us see through three aspects, password setting habits, password fatigue and the security risk of password reuse. We would go through the data that have been collected to come up with related situations and discussions.

Related Works

The current authenticating system has a negative impact on password security to some extent. In Gaw and Delten's work *Password Management Strategies for Online Accounts*, it has been argued that the password authentication system making the authenticating process more complex, has forced users to choose an easy but less secure password by, for example, shortening or using memory-friendly passwords [5].

The nature of text-based has also caused the potential security risks of passwords. In *Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat*, Pearman

er al. has discovered that the characters of text-based passwords impact users' password habits [6]. The concept of password fatigue is not used in this work, but the characters of passwords that lead to passwords reuses mentioned in the findings of this research are essentially the main factors that cause password fatigue. Such characters include password's complexity, password length, and the number of passwords.

Das er al.' work focuses on the interrelationship between password habits and account security. They found that password reuse significantly increased the security risk across accounts in their work *The Tangled Web of Password Reuse* [7]. Attackers are more likely to guess users' other accounts' passwords based on users' password habits using a leaked password. The password reuse can cause greater loss in this case.

In contrast to Das er al. 's work, this research focuses on the relationship between users' passwords habits and password security. I collect users' responses on their password behavior to explore the current status of users' awareness and practice of password security, from which we can discover the logical connections between users' password habits, password fatigue, and password reuse.

Chapter 3

METHODOLOGY

Choosing Methodology: Why Come up with a Survey?

The process of this research includes the data collection section and data analysis section. Since the goal of this research is to study the people's password security issue, it is necessary to collect a certain amount of data about users' password usage to help us better understand the current password usage situation and to support our following analysis. Therefore, a survey is needed for this research and I developed a questionnaire for data collection. The survey is designed to obtain the information from three perspectives: password setting habits, the experience of password fatigue and repeated password usage situation for multiple accounts. With the information obtained, the most common issue in password surety can be found.

In the analysis section, I will present the respondents' answers to the questionnaire to find the current situation of users' password risks. Each question will be discussed independently, and tables and pie charts will be used to present the results. Further, based on the results for each individual question, I will analysis the logic connections behind these answers. The goal of the analysis is to discover the casual relationship between users' password habits and security risks.

Data Collection: Why and How to do that?

The Design of the Questionnaire and the Design of the Questions

The questionnaire contains 10 questions, and the design of the questions is based on three aspects: Password setting habits (Questions 1- 4), Password fatigue (Questions 5-6), and Password reuse (Questions 7-10).

Password Setting Habits

knowing and summarizing the habitual way of how people generate their passwords will give us the most direct view of observing passwords in their natural habits. Because people are using some habitual ways to set their passwords for so many online accounts, it could lead to password fatigue. People are tired of passwords so much so that the term "password fatigue" has been developed to describe modern attitudes towards the login process.

Password Fatigue

Password fatigue is the feeling experienced by many people who are required to remember an excessive number of passwords as part of their daily routine, such as to set up a membership for Targets or Costco online, login to a computer at work, register for a new online service like Verizon or set up a bank account. It exists in our everyday life so commonly that it could lead to the results of severe password reuse.

Password Reuse

Because of the password reuse, it could lead to severe security problems [8]. Through some basic conversations with my friends, I found out that plenty of people have the habit of using the same password for many personal accounts. In this paper, I want to find out what is the possible possibility of people using the same password in all accounts located in various kinds of websites and applications.

Therefore, combined with the survey results, I want to compare the risk of choosing own passwords with using the same password in multiple accounts in different research papers and draw up a conclusion. Question 1 to 4 are related to respondents' text-based password generating habits. Each question reflects one particular important aspect of the generating habits. Q1 is related to the composing habit of passwords. Q2 reflects the password preference in relation to the habit of memorizing. Q3 explores the password complicity. And the password categorization habits are included in Q4. Question 5 and Question 6 are designed to understand the situation of password fatigue. Question 5 describes a general experience of users' password fatigue, and Question 6 explores the impact of password fatigue on users. The goal of Question 7 to Question 10 is to understand the current situation of password reuse. Question 7 is designed to understand the users' password diversity preference for managing multiple accounts. Question 8 discovers users' password categorization habits. In Question 9, I try to find the users' password storage habits when using browsers with the function of password saving. In Question 10, I want to discover the users' self-awareness of the risk of password reuse.

Sample Reliability Control: Sample Filtering, Avoidance of Biases and Random Selection Method

The reliability of the research results and analysis are largely dependent on the credibility of the sample, so it is important that the sample I use can truly reflect users' preference. In order to eliminate the interference of invalid samples and reduce potential bias, I designed the following steps to ensure the validity of the samples.

First, I consider the minimum answer time of the sample. Because the average reading speed for English native readers is 238 word per minute (wpm) for non-fiction and 260 word per minute for fiction [9] and the question part of the questionnaire contains 248 words, the invalid sample, it is unreasonable for the respondents to carefully read and

answer the questions with a time that far lower than 1 minute. There were 175 questionnaires collected in total. Therefore, the samples with the answer time lower than 1 minute which is 33 in total will be disregarded. Second, I use random selection method for the rest of the 142 samples to reduce the influence of gender bias, occupation bias and age bias. Because the questionnaire was sent out separately to different groups at different times, it is possible that a certain sequence of the answers is provided by a particular group of people, such as college students, aged people, programmers etc. This situation could potentially create gender bias, occupation bias, or age bias of the research. Therefore, I randomly picked 120 samples from 142 collected questionnaires to avoid the potential influence of the above biases.

Table 1 Average Reading Rate for English Native Readers.

Reading Material	Fiction	Non-Fiction
Reading Rate (words per minute)	238	260

Data Analysis Approach

With the data collected from the survey, I am also interested in exploring the logic connections behind the questions. Are there any cross relationships among password setting habits, password fatigue, and password reuse? I compared the answers to each of the two questions in the questionnaire to see if there was a correlation between answers. And I will discuss the logic behind the questions and find the interrelationship of answers if there is any. The findings in this section will further help us to provide reasonable and practical recommendations for the enhancement of users' password security.

Chapter 4

RESULTS & DISCUSSIONS

Totally, I collected 175 answers. 33 answers have the answer time lower than 1 minutes. After removing the invalid answers, the number of samples in the poll is 142. And then, to avoid biases as mentioned in the previous section, we randomly selected 120 answers and applied to the study. In this section, I will present the answer of each question independently. Then I will discuss the findings based on respondents' answers. According to each question, I analyzed based on its results and gave out my findings, issue, discussion and recommendations.

Question 1- 4: Password Setting Habits: Result details & Discussions

The result of Question 1- 4 is shown below. Those questions discover users' habitual way of how they prefer to generate their passwords.

Question 1

1. Do you normally create your own password or use the suggested auto-generated password by web browser?
A. Create my own.
B. I use the website suggested password.

Question 1 asks about users' password generating habits. The result of Question 1 is shown below. Among selected 120 respondents, 110 of them (92%) declared that they prefer setting passwords on their own, while only 10 respondents (8%) use website suggested passwords.

The reason people do not adopt auto-generated passwords may differ. Because auto-generated password function is usually provided by the browsers, instead of websites or service providers, therefore, users may not be able to have auto-generated due to technical constraints. Also, people may have a bias believing the auto-regenerated passwords are not secure as they are provided by other parties, however, actually the auto-regenerated passwords are relatively safer than self-generated passwords since they do not contain users' personal information and they are mostly irregular.

There is a clear tendency that people prefer to generate their own password. However, it may not be aware that the personalized passwords may have higher risk due to people may have their passwords related to their personal information such as birthday, name, or some special date. We will further explore this situation in the following content.

Question 2

2. If you are creating your own password, is it more likely to be related with birthday, name, ID no. or address kind of personal information?

A. Yes, it's related to personal information.

B. No, it's nothing related to my personal info.

C. I use the website suggested password.

Question 2 discovers the users' password generating preference. Among 120 samples, 49 respondents (41%) have their passwords to be related to their personal information, while 64 respondents (53%) avoid using personal information in password creation and 7 of them (6%) use website suggested passwords.

It is good to see that more than half of participants avoid using passwords containing personal information. However, the rest approximately 41% of people should now pay attention to their password generating habits. Commonly, people use their personal information in their password to help memory. But, such personal-information-related passwords are subject to higher possibility of cracking. Passwords containing personal information are more easily to be creaked. It is especially important for users to avoid using birthday, address, ID, and close relatives' information in their password.

Question 3

3. When setting up your password, do you often combine letters, numbers and special characters as higher password strength for safety?
A. Yes, I would prefer to use a complicated password like more than three types of characters combined.
B. No, I would prefer simple passwords such as only numbers or letters or combined because they are easier to remember.
C. I use the website suggested password.

Question 3 is also related to users' password generating preference. According to Question 3, we can see that the number of participants using complicated passwords (more than three types of characters combined) is 80 (67%), and the number of participants who prefer simple passwords is 33 (28%). 5 participants (5%) are using suggested passwords.

From the result, we can see that there is still a large portion of people choosing to use relatively fewer complex passwords for their accounts. What should be noticed is that the complexity of the password is another crucial determinant of password security. Generally, the more complex the passwords are, the safer the password can be. Every time there is an extra letter or symbol added to the password, the time taken to crack it increases exponentially. The relationship between the number of characters and the approximate amount of time to crack passwords can be seen from the chart below [10].

Table 2 Estimating Password Cracking Times by Characters.

7 characters	0.29 milliseconds
8 characters	5 hours
9 characters	5 days
10 characters	4 months
11 characters	1 decade
12 characters	2 centuries

The cost-performance of crack drop dramatically when the password contains 10 or more characters. Thus, it is recommended that the users set their passwords with a minimum of 10 characters to ensure their passwords' security in front of brute-force attack.

Question 4

4. Do you set separate passwords for your routine website accounts and the important accounts such as bank, SSN, school, etc.? *A. Yes, I set unique and specific passwords for my important accounts.* *B. No, I still use random passwords for my important accounts just like normal website accounts.*

Question 4 focuses on the password management habits of users. From the 120 respondents' answers on question 4, 80 respondents (67%) use separate passwords for different kinds of accounts, and the rest 40 of them (33%) do not separate their passwords.

Most respondents do understand the importance of separating passwords. However, people do not separate accounts mainly because managing an excessive number of passwords challenges their memory. The good point of separating passwords is that it can help users avoid further loss after one of the account passwords is leaked. Therefore, for security reasons, it is still recommended to use separate passwords for different accounts, especially for users' important accounts.

Question 5- 6: Password Fatigue: Result details & Discussions

Password fatigue is a term that describes users' modern attitudes towards the login process. Question 5 and Question 6 explore the current circumstance of password fatigue and users' attitudes toward it.

Question 5

5. Have you ever experienced Password Fatigue (the feeling experienced by many people who are required to remember an excessive number of passwords as part of their daily routine)?

A. Yes

B. No

C. Sometimes

Question 5 explores users' experience of password fatigue. In Question 5, 81 respondents (68%) reflect that they have experienced password fatigue when managing multiple passwords, while 32 respondents (27%) have not experienced password fatigue, and 7 respondents (5%) experience password fatigue occasionally.

More than half of respondents have the experience of password fatigue, which indicates the password fatigue is a common phenomenon in users' password management. The password fatigue is people inertia and exhaustion of managing passwords. As users are having more and more accounts that require text-based passwords on the internet, it is reasonable to infer that password fatigue will become even more common than today in the future. Because of the nature of the text-based password, password fatigue is somehow unavoidable.

Biometric passwords, such as fingerprint, face, voice, may offer a bright future of password management by providing more secure and convenient ways for the authentication process. Theoretically, human's biological characteristics are unique, and not replicable, so it can be safer if they are used for authentication. More importantly, users do not need to create a long chain of passwords for safety because they are the passwords themselves. We have witnessed a rapid development of biometric passwords in these years.

Now most smartphones can be unlocked using fingerprint or facial recognition. It is foreseeable that most of our social media accounts, bank accounts, and shopping accounts will adopt biometric authentication soon.

Question 6

6. After suffering with Password Fatigue, are you deciding to stick to using different passwords or reuse the same password for multiple accounts?
A. I don't mind, still decide to come up with different passwords for all my accounts.
B. I hate memorizing all those passwords, I decide to use only a few fixed passwords.
C. I use the website suggested passwords, so it doesn't matter to me.

Question 6 explores the impact of password fatigue on people's password habits. 43 respondents (36%) reflected that they are not affected by password fatigue, while 70 respondents (58%) decided to reduce the number of passwords after experiencing password fatigue, and 7 participants (6%) are not affected since they are using website suggested passwords.

It can be found that password fatigue may have a negative impact on users' password habits. From the result, we can infer that people tend to reduce the number of passwords for their account as a result of password fatigue. The excessive number of passwords that are needed to be managed can be a major cause of password fatigue. Studying password fatigue and the ways to avoid password fatigue can help promote password security. One of the future extensions of this research can focus on the relationship between users' password preference and password fatigue.

Question 7- 10: Password Reuse: Result details & Discussions

Password reuse is the users' tendency of using some same fixed password for multiple accounts. Question 7 to 10 discover users' current tendency of password reuse.

Question 7

7. Do you normally use only a few similar passwords for multiple personal accounts?
A. Yes, 1-2.
B. Yes, 3-4.
C. Yes, but more than 5.
D. No. I use whole different passwords for various websites and accounts.

Question 7 asks about uses' the general preference of password reuse. 29 respondents (24%) only use 1-2 passwords for multiple personal accounts. 50 respondents (42%) use 3-4 passwords for their accounts. 19 respondents (16%) have more than 5 passwords. And 22 respondents (18%) set different passwords for different accounts.

Around 82% of respondents have more or less been involved in password reuse, which increases the risks of account security for them. Again, the root of this issue comes from an obvious shortcoming of the text-based password. For users, the more the amount their password is, the higher the possibility of forgetting or losing password are, which will cause password fatigue, and eventually lead to password reuse. As mentioned above, this issue is caused by the nature of the text-based password and can hardly be avoided. Exploring new types of password can be the only way to address this issue.

Question 8

8. Do you categorize your passwords as social media, groceries, online shopping, etc. and use the same password for the similar accounts?

A. Yes, I use the same password for all similar kinds of accounts.

B. No, I use a few fixed passwords no matter what account.

C. No, I use all different passwords for various accounts.

Question 8 discovers the password categorizing habits of users. From the result of question 8, 36 participants (30%) create passwords based on the types of the account. 52 respondents (43%) do not categorize their password and use the same passwords for all kinds of accounts. Only 32 respondents (27%) use different passwords for each account.

It can be concluded that more than 70% of respondents have, to some extent, a password reuse situation. This is totally understandable. Based on a survey conducted in 2020, globally, the average number of social media accounts held by an internet user is 8.5. It is hard and painful for users to remember 8 passwords, not to mention their other types of accounts [11]. Under this circumstance, categorization is a good strategy that balances the users' preferences and security. For example, when a user's twitter account is cracked, although it means all of his social media accounts are endangered, at least his bank accounts are temporarily safe.

Question 9

9. After setting up a few fixed passwords, do you often choose to 'Save Password' on the Internet?

A. Yes

B. No

Question 9 is related to the users' password habit concerning password reuse. 66 respondents (55%) answer "Yes" when they were asking whether they would save the password in their browsers. And 54 participants (45%) would not save their passwords in their browsers.

From this question, it can be seen that people's attitude towards "save password" is unclear. "save password" is a function, which is commonly called password manager, provided by browsers or independent applications. It encrypts and saves users' passwords; users can use his passwords on other platforms by simply login to his password manager once. The security of password managers is controversial. Especially for online based password managers, since the passwords are saved on cloud, it increases the risk of password being leaked. The good side of password managers is also significant. First, it creates more convenience for users as it could autofill the passwords. Users can login to their accounts across-devices using only one password. Second, it allows users to create more complicated passwords without the worry of forgetting passwords. Besides, some password managers offer security alert functions that warn users their potential risks of passwords. The reliability of password managers remains to be proven by time.

Question 10

10. Are you aware of the potential security risk for reusing the same passwords for multiple accounts on the Internet?

A. Yes, I know the risk that reusing the same password may cause my several accounts being broken down at the same time. But I don't mind or I don't want to think about it.

B. No, I don't know that it may pose a severe security risk.

In the 10th question, I collected the users' response on their awareness of the risk of password reuse. 90 respondents (75%) understand the risks of password reuse. 30 respondents (25%) have a negative answer when they were asking about the awareness of password reuse.

It has to be pointed out that among 75% of participants whose answer is A, two types of people are included in this group. Some of them understand the risks of password reuse but don't mind the risk because they have consummate password management habits, therefore, they don't worry about their password security. For the other part of this group, they are aware of the risks of password reuse, but they choose to neglect it because of the influence of password fatigue. Therefore, it is imprecise to conclude that the awareness of the risks of password reuse leads to better password security conditions from the answers of this question because the above two groups in the option A are not distinguished.

Although more than half of respondents understand the potential security risk of password reuse, there are still a large portion of people who still haven't realized the risks. Once attackers break one of the accounts, they can easily access users' other accounts if users reuse their passwords. One feasible enhancement for password reuse is to ask developers to add a warning message about the password reuse when users create passwords.

The Exploration of Logical Connections Behind the Answers

For us to better understand the relationship among users' passwords setting habits, password fatigue, password reuse, and their impacts on password security, it is instrumental to explore the interrelation between users' answers of each question.

One important finding is that it can be observed there is a correlation between password fatigue and users' password habits. For example, Among 81 respondents who

declared they have experienced password fatigue in Question 5, 28 of them (35%) choose to keep using different passwords for different accounts in Question 6, while 50 of them (62%) reduce the amount of passwords and reuse the passwords for different accounts, and the rest 3 of them (3%) are using website suggested passwords.

This finding is consistent with our perception. The people who have the experience of password fatigue tend to reuse passwords for different accounts, which endanger their password security. It can be inferred that to enhance password security conditions, it is important to reduce the influence of password fatigue. Addressing password fatigue issues can be achieved by enhancing user experience in managing passwords. For example, CAPTCHA is a challenge-response test that is used to verify if the user trying to login is human or a robot. However, CAPTCHA is sometimes too complicated for users to answer, and it makes the login process even harder. Avoiding CAPTCHA being too hard then can be a practical way to enhance user experience.

Another interesting finding is that I do not observe a clear interrelationship between the awareness of the risk of password reuse and the practice of password reuse. I analyzed the answers of participants who state they are aware of the potential security risk for reusing the same passwords for multiple accounts on the Internet. Their answers in Question 7, 8, 9 are well-distributed, and there is not a clear tendency showing the influence of the awareness of the risk on them.

However, this does not mean the awareness of password security is not important. One possible explanation is that password fatigue also affects users' behaviors. Password fatigue is preventing users from choosing more secure but more complicated password practice. What we can learn from the analysis is that besides arousing users' awareness of password security, it is also important to build an environment where the users' experience and password security can be balanced.

Chapter 5

CONCLUSIONS

The Potential Improvements

From the answers obtained from the survey, we can see that people have a natural tendency to simplify their login process either by using short and easy passwords or reusing the same passwords for multiple accounts on the internet. These behaviors can lead to more risks for users' password security. The ignorance of risks and password fatigue are the major causes of users' unsecured password habits. Moreover, someone may understand the importance of passwords, but he knows little about what the correct and secure password habits are.

It also can be concluded that the condition of users' password setting habits is not optimistic. There still a large portion of users having unsecure password habits, such as using over-simplified passwords, password reuse, and avoiding changing passwords regularly. Those habits increase the risks of password security significantly. It is recommended that elementary education should incorporate the knowledge of information security, including password security, so that users can develop good password habits from an early age. Besides, it also can be effective if services providers or developers add a warning message or instruction about password security.

The Deficiencies of Text-based Password

From the analysis, it can be concluded that the nature defects of text-based password lead to password fatigue. For users, the text-based passwords are not memory-

friendly. It is difficult for users to manage multiple accounts with different passwords. It is also a burden for users to change passwords regularly. Therefore, password fatigue happens, and it leads to password reuse. Given that the users failed to manage their passwords, the account security risk raises.

The invention of new types of passwords can effectively reduce the occurrence of password fatigue. Biometric identification can provide a more convenient way for users' login process. With biometric password, such as fingerprint or facial identification, users can complete the authentication process with only one touch or just need to show in the camera for a second. More importantly, they don't need to memorize the passwords, which may earn more users' preference. But there are still hard-ware or soft-ware constraints for the use of biometric identification. Fingerprints, for example, require special readers which may not be supported by users' devices.

It can be sure that the future trend of the passwords is being more convenient and secure. But for now, while the text-based password is still the mainstream of the authentication tool, users still need to overcome their bad password habit and be aware of their password security.

REFENENCES

[1] [4] [6] S. Pearman, J. Thomas, P. E. Naeini, H. Habib, L. Bauer, N. Christin, L. F. Cranor, S. Egelman, and A. Forget, "Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat," *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA, 2017

[2] K. P.L. Coopamootoo, T. Gross, M. F. Partama, "An Empirical Investigation of Security Fatigue The Case of Password Choice after Solving a CAPTCHA," *Proceedings of the Learning from Authoritative Security Experiments Results (LASER) 2017*, Arlington, VA, USA

[3] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, R. Biddle, "Multiple Password Interference in Text Passwords and Click-based Graphical Passwords," CCS '09: *Proceedings of the 16th ACM conference on Computer and communications security*, Pp. 500-511, USA, November 2009

[5] S. Gaw, and E. W. Felten, "Password Management Strategies For Online Accounts," SOUPS 2006, pp. 44-55, USA, 2006

[7] A. Das, J. Bonneau, M. Caesar, N. Borisov, X. Wang, "The Tangled Web of Password Reuse," *Proceedings of the 2014 Network and Distributed System Security Symposium 2014*, USA, 2014

[8] B. Ives, K. Walsh, H. Schneider, "The Domino Effect of Password Reuse," *Communication of the ACM*, Vol.47, Pp. 75-78. 2004

[9] M. Brysbaert, "How many words do we read per minute? A review and meta-analysis of reading rate," *Journal of Memory and Language*, Volume 109, Amsterdam, Netherlands, December 2019

[10] BetterByus, "Estimating Password Cracking Times," Retrieved from: https://www.betterbuys.com/estimating-password-cracking-times/

[11] J. Clement, "Global social media account ownership from 2013 to 2018," April 2020, Retrieved from: https://www.statista.com/statistics/788084/number-of-social-media-accounts/