EMPIRICAL ANALYSIS ON THE USABILITY AND SECURITY OF PASSWORDS

A Project

Presented to the faculty of the Department of Computer Science

California State University, Sacramento

Submitted in partial satisfaction of
the requirements for the degree of

MASTER OF SCIENCE

in

Computer Science

by

Shweta Shenoy

SPRING
2019

EMPIRICAL ANALYSIS ON THE USABILITY AND SECURITY OF PASSWORDS

A Project

by

Shweta Shenoy

Approved by:

_____, Committee Chair
Yuan Cheng, Ph.D.

_____, Second Reader
Anna Baynes, Ph.D.

_____
Date

Student: Shweta Shenoy

I certify that this student has met the requirements for format contained in the University format manual, and that this project is suitable for shelving in the Library and credit is to be awarded for the project.

_____, Graduate Coordinator _____
Jinsong Ouyang, Ph.D. Date

Department of Computer Science

Abstract

of

EMPIRICAL ANALYSIS ON THE USABILITY AND SECURITY OF PASSWORDS

by

Shweta Shenoy

Security and usability have been on the opposite ends of the spectrum; sometimes, to achieve one, the other must be compromised to some extent. Passwords are a typical example in which usability, psychology, and security meet. Absurd password rules force users to create complex passwords for the sake of enhanced security. However, users often struggle to create and recall such passwords and resort to techniques such as writing them down, reusing them, and storing them in vulnerable ways. The use and management of passwords have become one of the biggest challenges for users and security experts today.

The strength of a password directly correlates to its security. In addition, we define the pronunciability of a password as a means to measure how easy it is to memorize – an aspect we associate with usability. These metrics, along with the opinions of real users from an online survey, will be used to empirically analyze the relationship between usability and security in user passwords.

This project analyzes a dataset of 300,000 passwords, to determine whether the user-generated passwords are both usable and secure. By quantifying the password strength and predicting the pronunciability of a password, we design a framework to map the relationship between the two.

We find that passwords are either secure or usable, but they rarely ace in both aspects. Furthermore, we suggest how password creation strategies can be adapted to better align with usable security.

_____, Committee Chair
Yuan Cheng, Ph.D.

_____
Date

DEDICATION

To my family

To my Professors

To my friends

ACKNOWLEDGMENTS

This work would not have been possible without the constant support and guidance of my project guide Dr. Yuan Cheng. As my professor and a mentor, you have been patiently guiding me from the past two years on this project as well as with courses related to Information and Computer Security. It was only due to your expertise and involvement that this project found direction; hence I am able to present this paper proudly. Thank you, Dr. Cheng.

I am grateful to Dr. Anna Baynes, my second reader, for your support and feedback on my work. I cannot thank you enough for your quick responses, your helpful, and approachable nature.

I am especially indebted to Dr. Jinsong Ouyang, our graduate coordinator and the Department of Computer Science at CSU, Sacramento, for going beyond their responsibilities as professors to guide and provide opportunities to students to help them excel in their educational and career goals.

Nobody has been more important to me in the pursuit of this project than the members of my family. I want to thank my parents and sister, whose love and guidance are with me in everything I pursue. Last but not least, I am grateful to my loving and supportive friends, for proof-reading my work and providing suggestions and advice throughout my project. Thank you.

TABLE OF CONTENTS

Page

LIST OF TABLES

Tables Page

LIST OF FIGURES

Figures Page

CHAPTER 1

INTRODUCTION

Passwords are not the most convenient way to authenticate yourself, and neither are they inherently secure [1]. Especially with the increasing demands associated with their creation, *passwords* no longer remain simple *words*. Consequently, people fall prey to insecure practices, such as scribbling the passwords on paper, reusing them across different accounts [2-4], or creating passwords that are easily guessed [2, 3]. A plausible rationale for such practices are the stringent password creation policies. They make it challenging for users to create passwords, but do they at least guarantee secure and strong passwords?

Some of the most prevalent password requirements adopted by organizations and applications include,

- Passwords must exceed a minimum length and fall below a maximum length. The average required length is around 8 – 12 characters.
- They must contain a combination of uppercase and lowercase letters, numbers, and special characters – often chosen from a limited set defined by the organization. It usually excludes certain characters such as '~', '>', '<', '{', '}'.
- They should not contain common dictionary words, substrings of their username, or the name of the application.

Studies show that there is little rationale on why organizations prefer to use these policies [4]. In fact, it is difficult to determine a universal standard as different

organizations and applications enforce different password creation rules. Studies show that even the most popular guidelines are based on theoretical estimates [5, 6] or small-scale research studies [7, 8].

Historically, these policies were believed to be adequate and were implemented to help prevent password guessing attacks [9]. In those times, computational power was far scarcer, and passwords were not as large of a foothold to adversaries as it is today. Thus, these policies seemed to be reasonable at providing users with some degree of security. Furthermore, these password creation policies act as a fail-safe mechanism to at least prevent users from creating extremely vulnerable passwords and add a layer of complexity to a primary password. Many researchers support the new guidelines published by the National Institute of Standards and Technologies (NIST). It recommends eliminating or reducing complex rules, such as allowing all printable characters – including white spaces, increasing the maximum length to 64 characters and not requiring special characters [6]. However, very few organizations have implemented these guidelines. As a result, strict password policies are still a widespread practice today.

Passwords are supplemented by other authentication methods, such as fingerprint and face recognition, but they are merely an adjunct to passwords, not a replacement. Security experts claim that biometrics are used for ease of access to systems; on the other hand, passwords are used to establish the initial trusted relationship, and as a fall back when the biometrics fail [10]. In fact, the amount of risk a compromised password constitutes depends on how it is used and what it is protecting. Alternatively, a stronger authentication method, such as biometrics, might not be cost-effective with low-value resources [10].

Therefore, we will always resort back to text-based passwords. To balance the convenience of use for users as well as protect their privacy, it is crucial that passwords are both usable and secure. In an effort to combat the inherent and user-induced risks and weaknesses, organizations and applications institute these rules or password creation policies, to which users must comply when creating passwords.

The fundamental objective of usable security is to develop security measures that respect human performance and their goals within a system. To achieve this, researchers focus on aligning aspects of human-computer interaction with elements of computer security. Although usability and security were thought to be inherently antagonistic, today there is broad consensus that systems that are not usable will eventually suffer security failures when they are deployed into the real world [11]. Only by simultaneously addressing both usability and security concerns will we be able to build genuinely secure systems.

1.1 Overview

Conducting user research is a fundamental component of studying usability. In our project, it helps us uncover popular opinions regarding the use and management of passwords. The first part of this project is an online user survey. The second part is quantifying and technically assessing the two facets of a password: usability and security. The two are first studied individually before analyzing them as one. The metrics chosen to analyze each component are discussed in detail in Chapters 3 and 4. Throughout the project, we use the survey responses to supplement the observations made through the

technical implementation. Together, the two allow us to make an unbiased conclusion. Figure 1 shows the high-level methodology of this project.

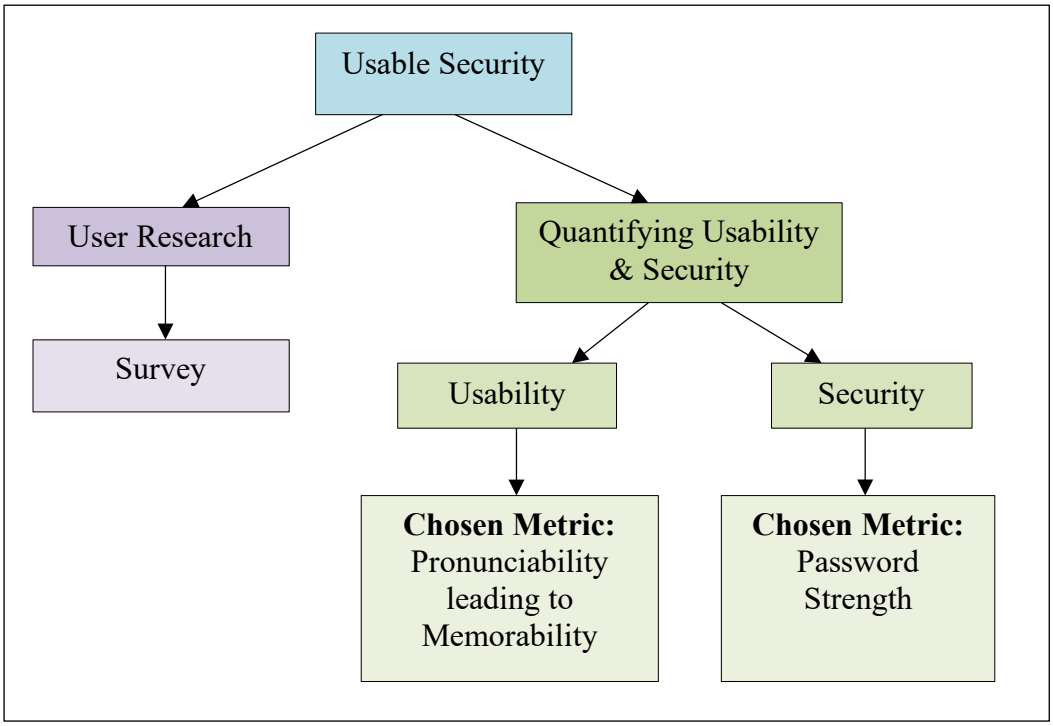

Figure 1: High-level overview of the project

1.2 Organization

The remainder of this report discusses the literature relevant to this study (Chapter 2) followed by the methodology used in investigating this problem (Chapters 3 and 4). Then, we present our findings regarding the usability and security of user-created passwords and security perceptions related to password creation policies (Chapter 5). Finally, we conclude with a discussion of our results (Chapter 6).

.

CHAPTER 2

LITERATURE REVIEW

The sole purpose and existence of passwords were to provide authentication; and as they became the first line of defense against intrusions, other attributes got associated with them, such as ease of use, and the need for strong, secure, and unique passwords. These factors colloquially form the field of usable security. There is an excellent body of existing work in this field and emerging within is the effort to solve the complexity and frustrations around passwords [2].

Several studies have examined how user-created passwords are not secure [5] and have related the lack of security to password creation policies [4]. These policies are a typical example of how conventional wisdom might be wrong, or rather, becoming irrelevant as the capability and computational power of our systems have changed. Originally, the purpose of asking users to include numbers and special characters into their passwords was to expand the password space, i.e., increase the number of unique passwords that can be created from a set of characters. However, most people respond to such complex policies by taking their existing passwords and modifying them so that they meet the minimum requirements. For example, "password" becomes "P@$$w0rd!", or even "P@$$w0rdP@$$w0rd!" to meet all the requirements [8]. Adversaries have quickly caught on with the trends of substituting letters with matching characters or making other modification to dictionary words, and have now devised systems that look for all possible changes to dictionary words to crack passwords. Our study contributes to this field of

research by providing more reasoning to question the merits of these existing policies and encourages a shift from these longstanding ways to better techniques acquiescent with user convenience and security.

Other studies dwell upon the mathematical aspects of security and passwords – such as its entropy [4], statistical analysis, and possibilities of attacks based on the password space [9]. Entropy has commonly been used as a measure of password strength. The calculation takes into account the length of a password and the number of different character classes it uses to generate entropy [4]. This means that the higher the entropy, the more random and hence more secure the password is. These estimates, although theoretically correct, are not an accurate representation of strength as users do not actually choose such random characters in their passwords [5]. They merely decorate dictionary words as previously explained. These lead to the creation of strength meters, some of which evaluate a password and provide an approximate number of attempts required for a given password to be guessed. These strength meters usually rate passwords on a scale of very-weak to very-strong. In our research, we further the concept of strength meters and add a usability aspect to the otherwise used as a strength only calculator. We analyze where the majority of the user-created passwords fall on the strength meter and propose empirical observations on the results.

Some studies dive deep into the usability and user experience aspect of passwords, conduct surveys and interviews, and examine the psychology of humans behind password selection [9, 4]. Although it is challenging to generalize human cognition based on a

surveyed sample, it provides excellent insight to security professionals on how to strike a balance between security and usability.

Even if we assume that password policies result in stronger passwords, they make those passwords difficult to remember or type. There are only a few published materials that study the ease and convenience of using and remembering strong passwords. Most related to our study is the research that combines the ease of memorability of passwords with its security. For example, Kelley et al. conducted a study where the users were shown passwords of varying complexity for a certain amount of time, after which they were to reproduce all the passwords they could remember [12]. Out of the ones they remembered, the researchers would evaluate how secure and memorable passwords are. The results, perhaps not surprisingly, were that users could easily remember words and sentences as opposed to random strings of characters.

This study focuses on the relationship between usability and security in user-created passwords by exploring a different approach to solve the password problem. We aim to advance the understanding of the factors that make creating and remembering strong passwords difficult and hypothesize based on the empirical evidence that as the security of passwords is forced to increase, the usability decreases.

There are certain facets of passwords that we do not consider in our study. The use of password management software could annul some of our findings [4]. We also do not have a baseline against which to evaluate the results. In general, human behavior is challenging to analyze technically and what might be usable according to our study might be different for others [13].

CHAPTER 3

PASSWORD SECURITY

In this chapter, we discuss how the strength of a password is a pertinent metric to understand password security. We develop a password strength calculator and use it to analyze user-created passwords.

3.1 Importance of Strong and Secure Passwords

The easiest foothold for adversaries to gain access to our systems is by cracking our passwords [14]. A strong password makes it prohibitively difficult for adversaries to break into a system and lowers the likelihood that our computers will fall victim to an unwanted intrusion [15]. The consequences for victims of such intrusions can be highly destructive and damaging. It could include loss of valuable data such as pictures, emails, or other personal information. Victims could also have their bank account information stolen, leading to financial fraud or even identity theft. The risks of a compromised password have too much at stake for it to be taken lightly. Moreover, modern technology has aided adversaries to brute-force passwords in a matter of a few seconds. To combat these weaknesses of text-based passwords and help users create strong passwords, organizations institute password policies to which users must adhere when creating a password. The challenge faced today is that the caliber of these policies designed to increase password security is in question [16, 17]. With all these policies in place, are user-created passwords actually secure?

3.2 Methodology

Password security can be evaluated using a few different methods. Principally, a password is a combination of a string of characters. Using a combination of mathematical reasoning, for example, combinatorics, and security principles [14] of what qualifies as a strong or a weak password, we design a password strength calculator. Many organizations and applications are using password strength meters to evaluate passwords predominantly and suggest where it ranks on a scale of weak to strong. Often, these strength meters will visually represent the strength of a password and will only allow successful password creation and updates if they satisfy all the requirements. Research has proven that these meters, in fact, help users in creating stronger passwords [7].

3.3 Dataset

In our study, we design a password strength calculator that evaluates how strong a password is based on the characters it contains. This strength calculator was used on a large dump of user-created passwords. The dataset used in this study was courtesy of Chun Wang et al., [18] who provided a dataset of 28,836,775 users and their passwords. Each user is identified by a unique user ID. For this study, we focused on 300,000 unique passwords from this dataset.

First, we categorized each password into one of the six categories from very-weak to very-strong or invalid. The general basis for this categorization is as shown in Table 1.

Table 1: Categorizing passwords into various categories to evaluate strength.

Assigned Strength	Quantifier	Attributes
0	Very Weak	Less than 6 characters
1	Weak	6 – 8 characters Lower case only Special characters
2	Average	6 – 8 characters Alphanumeric Special characters
3	Good	8 – 14 characters Alphanumeric Special characters
4	Very Strong	14 + characters
-1	Invalid	Invalid Symbols not recognized by the standard US English Keyboard

These categories complement current research in measuring password strength [2, 19] and are further backed by NIST's password guidelines [6]. The basis for these guidelines and categories can also be proven mathematically to limit chances of attacks such as a brute-force attack based on password length and characteristics [4]. Fundamentally, the more the characters, the larger the password space. A large password space generates exponential combinations of passwords and makes it impossible to be a victim of a brute-force attack.

Therefore, a password meeting some of the most commonly adapted password requirements, such as length, case, and special characters, would at best be categorized as a 3 or a good password. Whereas, a very-strong password is not one that has more special characters and numbers, but is a passphrase, or a long sentence [20]. A passphrase is not restricted by any requirements and in fact, even encouraged to include whitespaces. For

example, a password such as “FqDn!ty34” consisting of 9 characters, numbers, special characters, and a combination of upper and lower case alphabets will take at most four weeks to brute-force. However, a password such as "my dog is blue in color" with absolutely nothing but lower-case alphabets and white spaces will take up to 84 quintillion years to brute-force [21]. It is quite apparent which of the two passwords is more usable, but to reiterate, it is the latter. This goes to prove that a more complex password does not equal more security.

3.4 Distribution

To understand how user passwords range over these five categories, we plot a histogram with the distribution of the passwords in the dataset in Figure 2.

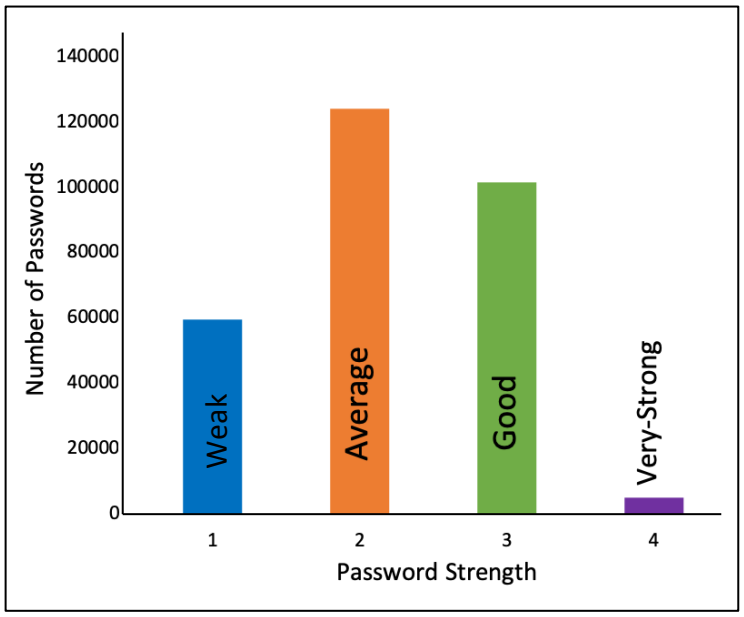

Figure 2: Distribution of Passwords

It is evident that most of the users choose average to good passwords and the concentration of very-strong passwords is low.

Although there could be numerous reasons for the plunge in strength in the very-strong category, based on the results of the survey, it is evident that users find it challenging to adhere to password creation policies that satisfy all requirements yet keeping it memorable. They express their annoyance caused by specific requirements for password creation and admit they circulate only a few different passwords across all services. This poses a significant security weakness as a compromise on one service could potentially lead to many other compromises. This figure also demonstrates that users are creating their passwords by satisfying only the minimum requirements, which is another reason for the significant fall in the distribution of the very-strong passwords.

CHAPTER 4

PASSWORD USABILITY

In this chapter, we will add the second aspect – usability, to identify how the strength of passwords affects the usability. We develop a framework to predict how pronounceable a password is and use it to measure usability.

4.1 User Survey

Keeping user convenience as the focus of the usability aspect of this study, we started the analysis by conducting a survey aimed primarily on collecting user responses about password creation policies. The participants were also asked to provide opinions about password management and hygiene. The survey was conducted on Amazon's Mechanical Turk platform with approval from the Institutional Review Board at California State University, Sacramento. All participants were 18 years or older of age and had a Human Intelligence Task (HITs) approval rate of over 90%. Another screening parameter was that every user had at least one main password to base their opinions off. A total of 100 responses were consolidated for the analysis.

It was evident from the survey that users feel forced to create complex passwords which they fear forgetting, especially when there are several to remember. Memorizing multiple passwords has been a recurrent struggle. Technically analyzing and quantifying how easy or difficult it is to memorize a password is a more significant challenge as memorability is a human cognitive function. Researchers typically examine memorability through interviews and surveys. This is essential as it provides qualitative information

about user experience which is not achievable through any amounts of technical implementations. However, it is also not possible to quantify how memorable user-created passwords are solely based on user responses. By quantifying memorability, we can more accurately comment on the effects of policies on the usability of passwords. In this paper, we present the first framework (we are aware of) to quantify the faculty of the human brain – memorability.

4.2 Phoneme Translation

Webster's dictionary defines the word *memorability* as the quality or state of being easy to remember. It implies that if something is easy to remember, then it can be easy to memorize. In this context, we define that a word is easy to remember and memorize if a person can pronounce it. This also applies to passwords. If a password can be pronounced, then it can be easy to remember. We define a pronounceable and thus memorable password as a usable password (Figure 3).

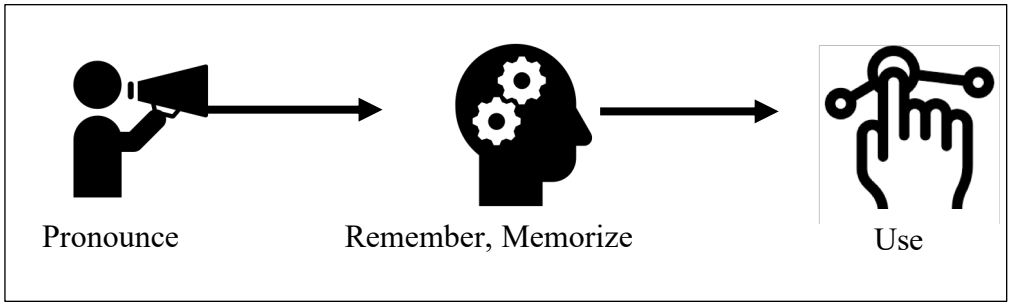

Figure 3: Pronunciability, Memorability and Usability

Our methodology is to develop a framework to predict how pronounceable a password is based on its *phoneme* representation. A phoneme is a unit of sound in speech. In other words, it is a perceptually distinct unit of sound that distinguishes one syllable from another. A set of phonemes form the sound representation of a word. For instance,

the phoneme representation of the word “password” is “p-ae-s-w-er-d" (based on CMU Pronouncing Dictionary [22]).

The use of phonemes is considered as an essential part of various speech synthesis and natural language processing techniques. The standard dictionary represents words in their phonetic representation, which is also a technique to analyze the sound of a word. However, phonetics fails to disambiguate the pronunciation of words that have multiple pronunciations, also known as homographs. Phonemes can detect similar-sounding words even when they are spelled differently and can also convert a numerical value, which technically can be pronounced, into phonemes. For these reasons, we used phonemes as a technique to measure pronunciability of a password.

Generally, text-based passwords are advised not to be plain dictionary words, although they will always have a spelling to represent it. Using that spelling we can convert it to its phoneme representation. The framework we designed can convert the spelling of a password to its pronunciation or, phoneme. For example, a string of words, such as “ApplesAndOranges,” can be represented using phonemes as “Ae-p-ah-l-z–Ah-n-d–Ao-r-ah-n-jh-ah-z.”

4.3 Set of Phonemes

The set of all phonemes were taken from the CMU Pronouncing Dictionary [22]. They have identified 39 phonemes for the English language. Advanced Research Projects Agency (ARPA), developed a set of phonetic transcription codes – ARPAbet, as a part of their speech understanding research project. The phoneme set used in this project was created based on the ARPAbet symbol set. It represents phonemes and allophones of the

standard American English with unique ASCII character sequences [23]. Overall, this set of phonemes consists of all possible pronunciations existing in the English language.

4.4 Methodology

First, we break down every password in the dataset into its phoneme representation. We then map the phonemes against the set of all possible phoneme combinations in the English language to predict the ease of memorability as demonstrated in Figure 4.

4.5 Fuzzy String-Matching

The phoneme representation of a password is then compared against the set of all phonemes using Python's fuzzywuzzy library [24]. Fuzzywuzzy is a string-matching algorithm that uses fuzzy string-matching and Levenshtein Distance [25] to calculate the differences between two strings. Fuzzy string-matching is the process of finding strings that match a given pattern approximately, and Levenshtein Distance is a method used to measure the differences between two strings.

Every password in the dataset will not match an existing phoneme exactly. The fuzzy string-matching technique is not only able to detect if two strings match, but also calculate how similar two strings are. For example, the word "medieval" can be represented phonematically as "m-ih0-d-iy1-v-ah0-l." Although, when choosing passwords, users can choose to spell it in many different ways, such as "medevel," "maideval," "midivl," etc. Each of these will be approximately matched to the existing phoneme combinations and scored based on how closely they map to existing phonemes. Additionally, the algorithm computes how similar or different it is from existing

phonemes and assigns a score. In the context of our project, this logic is applied to user-created passwords. Each password is fuzzy string-matched with existing phonemes in the English language to predict how pronounceable a password is.

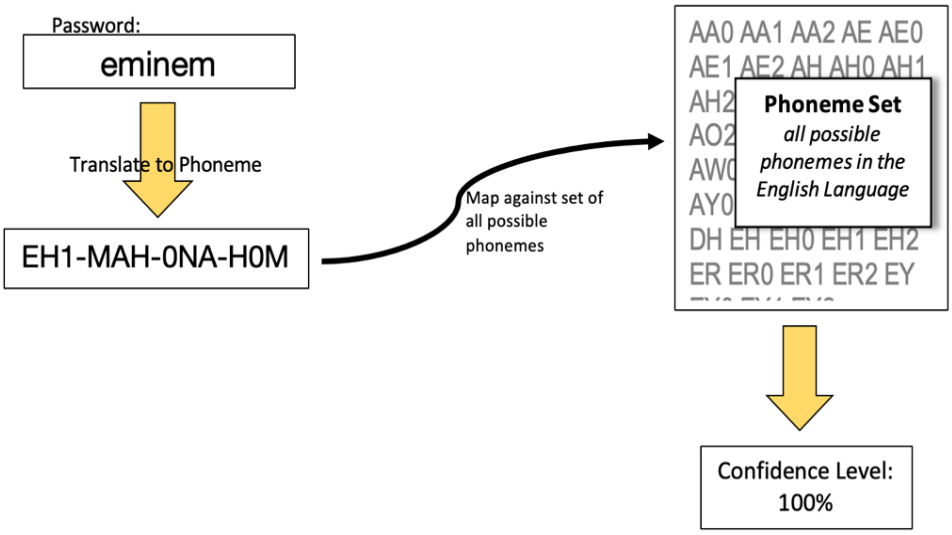

Figure 4: Phoneme Translation: an example to convert a password to its phonematic representation and predict its pronunciability.

Expanding on the example mentioned, Table 2 displays the phonemes and its predicted pronunciability for various versions of the same word. Here we have considered "medieval" to be the original word, and the words following it to be its versions. Though not real words, the phonemes of words 2, 3, and 4 are pronounceable in English. The original word has been used in this example to make a point in case, but in reality, the phonemes are not mapped against a particular word, but all possible combinations of phonemes. Similarly, all the passwords in the dataset are matched against the set of phonemes.

Table 2: Fuzzy string-matching example

No.	Word	Phoneme	Percent Pronounceable
1	Medieval	MIH0DIY1VAH0L	100%
2	Medevel	MEH1DIH0VAH0L	92%
3	Maideval	MEY1DAH0VAH0L	90%
4	Midivl	MIH1DIH0VAH0L	89%

After evaluating how similar two strings are, Fuzzywuzzy returns a similarity index out of 100. The similarity index is a percentage of confidence with which we can pronounce a password. A high confidence level indicates that the word is highly pronounceable, and a low confidence level indicates the opposite.

At the end of this implementation, every password in the dataset gets assigned a level of confidence. These confidence levels predict how pronounceable and hence how usable a password is. Using these two metrics, password strength and password pronunciability, we map a function of the two together.

CHAPTER 5

FINDINGS AND INTERPRETATIONS

In this chapter, all the experimental results from Chapters 3 and 4 are presented and examined in detail. We conclude this chapter with a discussion of our project, survey, and findings.

5.1 Combined Trends and Results

Specifically, we analyzed password security using a password strength calculator and password usability using pronunciability and memorability. The goal of this research was to empirically analyze usability and security in user-created passwords. We first calculated the strength of each password in the dataset and then assigned each with a predicted percentage of memorability. To analyze the two together, we map usability and security in Figure 5.

This figure displays the various strength categories (very-weak, weak, average, good, very-strong) on the x-axis and the mean value of pronunciability in each category on the y-axis. It is evident that the first two bars (very-weak and weak) are highly pronounceable, indicating to be highly usable. As the password strength increases to average and good, the mean value of pronunciability decreases. As the strength further increases to very-strong, there is a significant decrease in the value of pronunciability, indicating that very-strong passwords are not as usable.

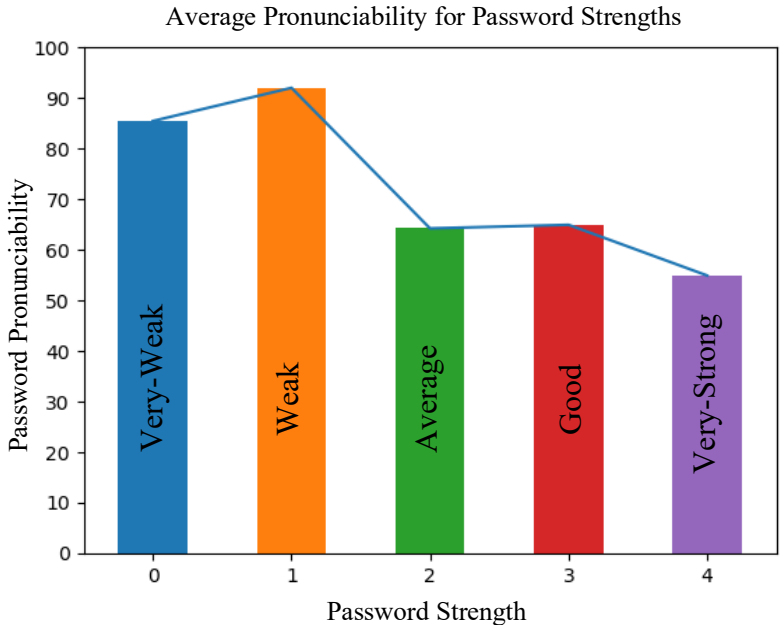

Figure 5: Usability and Strength

This goes to interpret that users fail to successfully create passwords that are both usable and secure. The few very-strong passwords that we have in this dataset have been compromised on its usability aspect for the sake of security and have a mean pronunciability value of only 55%.

Using the strength of a password as a metric associated with the security of the password and using the pronunciability as a metric associated with usability, from the data analyzed in our dataset, we observe that as the security of password increases, the usability decreases.

5.2 High Usability versus High Strength

To assess this observation further, we dig deeper into our results. Table 3 displays the top 50 passwords from the dataset that have a pronunciability of 100%. To reiterate, the field *pronunciability* in the table is a predicted measure of how pronounceable a

password is. The higher the percentage, the easier it is to pronounce and vice versa. Additionally, the easier it is to pronounce the password, the more memorable and usable it becomes.

Table 3: Top 50 passwords with high pronunciability (100% pronounceable).

Password	Pronunciability (%)	Strength	Password	Pronunciability (%)	Strength
beloved	100	1	jazzey	100	1
hollister	100	3	prakash	100	1
theman	100	1	adrian	100	1
nascar	100	1	eittah	100	1
hitchhiker	100	3	loveless	100	1
speakers	100	1	devon	100	0
kayla	100	0	flamingo	100	1
sexy	100	0	curtis	100	1
morning	100	1	angels	100	1
elefante	100	1	elliott	100	1
francia	100	1	rusty	100	0
shorty	100	1	Wallis	100	2
lover	100	0	ithaca	100	1
tule	100	0	michael	100	1
eminem	100	1	escape	100	1
warren	100	1	hunter	100	1
graeme	100	1	darren	100	1
alexander	100	3	password	100	1
smiles	100	1	diamond	100	1
armstrong	100	3	lacrosse	100	1
spiderman	100	3	love	100	0
whatever	100	1	rebelde	100	1
lexmark	100	1	ben	100	0
aliya	100	0	pasar	100	0
harriott	100	1	anam	100	0

Table 4: Count of passwords in each strength category from Table 3.

Strength	Count of Passwords
0 – Very-weak	11
1 – Weak	33
2 – Average	1
3 – Good	5
Grand Total	**50**

An apparent observation is the values in the strength field. Majority of the most-usable passwords are weak in strength. Out of the 50 most usable passwords, 44 of them are weak or very-weak (Table 4).

Similarly, Table 5 displays the top 50 passwords with the highest strength. The strongest passwords – considered 'very-strong,' are assigned a value of 4 via our strength calculator.

Table 5: Top 50 very-strong passwords (very-strong is assigned a value of 4).

Password	Pronunciability (%)	Strength
stereo0632176360	36	4
spyros0987654321	36	4
vfrchekbn9999999	36	4
summer280488888***	36	4
Zsoleszka1981070138	36	4
89872731020sveta	36	4
dogovor123456789	36	4
ASDFGH0987654321	37	4
alenchik16121992	37	4
t!t0_410714745	37	4
zxcvbnm123456789	37	4
password123456789	37	4
rimma89028681415	37	4
24121980arslanova	38	4
qwer123asdf456zxcv789	38	4
19931128azat-gim	39	4

patrickwii122406	39	4
model872trains543	39	4
AWESDRhujiok531983	39	4
MizerBek15081997	40	4
4764728AndreyAdamov	40	4
putskova14011985	40	4
fynbcgfvth159753	41	4
15132009gorlovka	41	4
krug_224krug_224	42	4
tigirans24011993	42	4
7534043kristinka	42	4
nostardamus524376	42	4
06748252cthufafy	42	4
197175:Dave:Smith	43	4
Mashulya30091990	43	4
vjkjnrjvgjvjhlt998821	43	4
HUNTERISCOOL12345	43	4
3643020sebastyan	43	4
121022:Felix:Arredondo	44	4
05041984alexandr	44	4
w68qw6b89438ilovejesus	44	4
babaroga00440044	46	4
bujh.irf01022008	47	4
felixalexreyes123	48	4
eronov8624kirill	50	4
rajdurgocharran0928	50	4
kiss*the/end7804	50	4
rjay2323@yahoo.com	51	4
systemofadown123	51	4
laurenspassword333	52	4
acer1987qwerty2007	52	4
uitarist2007@rambler.ru	52	4
creative@321.com	52	4
bizimov2005artem	53	4

Not surprisingly, the pronunciability of very-strong passwords is reasonably low. The 50 strongest passwords are barely 50% pronounceable. This ingeminates the struggles user face to create passwords that are both usable and strong.

5.3 Use of Passphrases

Bill Burr, the manager of NIST, and the original creator of complex password policies [26], recently mentioned in an interview with The Wall Street Journal [26] that he regrets the policies he originally published. In fact, now, Burr et al. at NIST recommend the use of passphrases as described in Chapter 3.4. In the dataset used for this project, the use of passphrases as passwords were very few. We discovered through the responses in the survey that a possible reason for this could be the unawareness among users regarding the benefits of using passphrases. Users in the survey are of the opinion that the more complex and stricter a password is, the more secure it is. Furthermore, the mandatory enforcement of some of the password creation policies prevents users from even creating a passphrase. For example, most applications limit the maximum length of a password to stay under 12 to 14 characters; and a passphrase is one with over 14 characters. Although limited in number, we analyzed the usability and security of the passphrases found in our dataset. Table 6 displays a list of 15 passphrases, with their predicted pronunciability and strength.

We find that users who used passphrases for passwords were successful in creating a very-strong (4) password. Additionally, the percentage of pronunciability of these passphrases are relatively high (90% and above). Out of all the user-created passwords in our dataset, the ones to excel in both usability and strength are passphrases.

Table 6: Filtering the dataset to display only passphrases.

Password	Pronunciability (%)	Strength
commercialista77	91	4
tasteslikechicken	100	4
happy_little_elf	100	4
PRINCIPLEPRINCIPLE	100	4
killerprostitute	100	4
MottoTondeMiso12	96	4
predictable_in_gold	100	4
carlosjamesantonio	97	4
mauricepauljones	100	4
awellrespectedman	100	4
moneyovereverything	100	4
associatedcontent	100	4
RedeemedByJESUS1	100	4
javierantoniocaleromendoza14	98	4
Lyrical_princess	100	4

5.4 Survey Findings

Our survey asked users their opinions on password hygiene, including password expiration, password creation, management, and its impact on security and usability. Similar to the participants in a study conducted by NIST [8], our participants expressed their frustrations with absurd password creation policies and their only available option – coping with this system.

Participants admitted resorting to the undesirable side effects of complex password requirements, such as writing passwords down and reusing them to avoid frequently forgetting them. The use of such insecure practices leads us to wonder whether the harm

caused by users complying with a restrictive password policy may be more than the good introduced by that policy [8].

Our results indicate that majority of the users still use techniques such as converting alphabets to characters, for example, the letter ‘e’ to ‘3’ and the letter ‘o’ to ‘0’ in order to make their passwords more secure. Unfortunately, users don’t seem to realize that these complex restrictions that they seem to be frustrated with are actually not providing them the security they are expecting.

5.2 Discussion

Researchers have used several experiments to question the merits of password creation policies. The metrics chosen in this study – password strength and pronunciability are a unique approach towards the solution to the password problem.

In this paper, we have discussed the existing password creation policies, the challenges it brings forth today, as well as the NIST published recommendations to invalidate or modify these complex policies. Although the newer and easier policy recommendations have been published for almost two years, they have not been adopted by many organizations.

The primary reason for this is due to the preconceived notion of security that users possess. It is believed that the more complex and harder something is, the more secure it probably is. In the survey conducted, users were asked to rate, on a scale of 1 – 5, their convenience with specific password creation policies, such as minimum/maximum length, use of numbers, and special characters. Here, a score of 1 would imply low convenience, and a score of 5 high convenience. For the questions related to this, the user’s responses

were 3 and below, indicating that these policies are not very convenient to use. Figure 6 shows that 59% of the users feel that password policies are not convenient to use (Strongly Disagree, Disagree). 25% of the user find it neutral and only 16% of the users find it convenient.

However, when asked if they believe these policies helped keep their passwords secure, most of the responses were ranked 3 and above. Figure 7 shows that 89% of the users believe (Agree, Strongly Agree) that existing password policies help strengthen and secure their passwords. This goes to prove that users abide with inconvenience and compromise on usability for the mere perception of security.

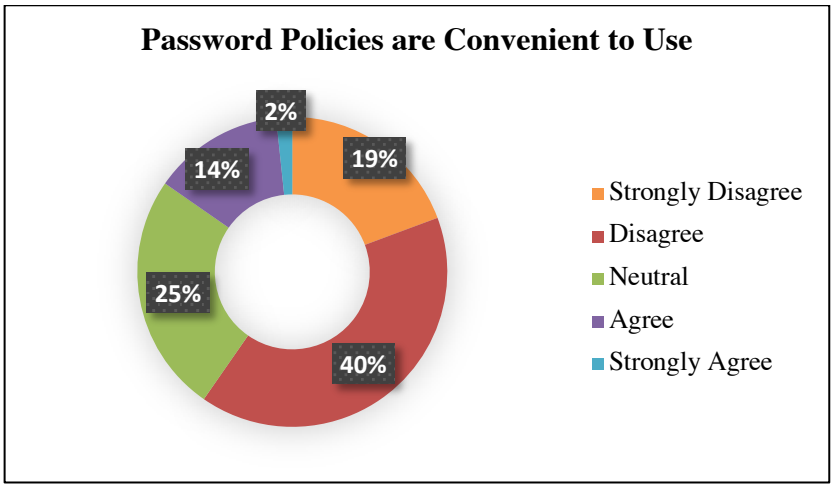

Figure 6: User responses: Combined results of questions asking if users find password policies convenient.

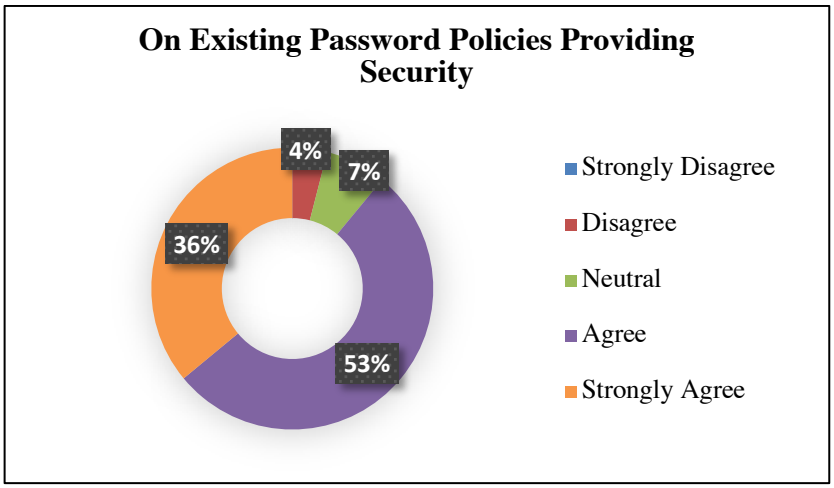

Figure 7: User responses: Existing password policies help strengthen and secure their passwords.

Our study confirms certain password convictions that are in practice today. An important fact iterated throughout this paper is that password management is a challenge for users; and the insecure password practices reported as a consequence of the former needs to be addressed. Although we cannot make specific password policy recommendations without further validation, we believe our results provide valuable insights that serve as indicators to improve existing password policies.

We also emphasize the importance and ease of using passphrases as passwords. Even as I say so, I myself am unable to use passphrases in most applications I use due to the password restrictions imposed during creation. However, based on the results of this study and the opinions of many security experts [1], we recommend organizations and applications to overcome the discussed preconceived notion of security and embrace the use of easier and more secure passphrases.

Always choosing the most stringent password composition policy may be disastrous, endangering both usability and security with no gains. We can see from our

results that only a few users have managed to create very-strong passwords (Figure 2). Even then, the usability of these passwords is low. Additionally, participants voiced the same through the survey. We recommend that organizations reconsider whether the policies they create are worth the minimal security gains if users will just find security-breaching turnarounds to evade complexity.

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 Conclusion

Password creation policies, such as the ones mentioned in the previous sections, are still widely practiced. These policies are potentially responsible for the lack of usability in passwords as well as employing insecure password practices that place a user's security at risk. Users claim that they find it challenging to comply with these policies and often find a way around them – such as reusing a password across different services to prevent remembering new ones, writing them down or even changing only a few characters from one password to another.

In this paper, we present an empirical analysis of the usability and security among user-created passwords. We calculate the strength of a password by developing a password strength calculator. It categorizes each password into one of these five categories: very-weak, weak, average, good, and very-strong. Next, we quantify the usability of passwords by predicting how pronounceable it is. We apply this to a dataset of 300,000 passwords and analyze it together with the responses gathered through an online survey on password opinions.

Based on our results, we agree with conjectures that the effectiveness of password creation policies is weak. Our study calls into question the continued use of these policies and provides empirical evidence to move towards passwords in line with usable security.

We define a unique approach to achieve usability – by studying the logic behind memorizing passwords. We analyze each password based on its pronunciation and predict its ease of memorability and usability. Our dataset allows us to have a reasonably comprehensive view of how most of the users aim to create usable passwords, but unfortunately, our password policies do not consider them to be secure. Whereas the passwords that are considered to be secure, people do not find them to be usable.

Passphrases are becoming a promising approach for user authentication to provide the level of security and usability ideally envisioned. However, we have to make our policies and enforcement tools conscious of the same. In support of this, we provide significant evidence and highlight the importance of shifting to this solution.

While validation is a challenge, we have made the first steps toward understanding the usability and security of user-created passwords.

6.2 Future Work

With respect to this research, certain limitations of the design could be improved in the future. For example, the current set of phonemes used can only accommodate pronunciations in the English language. This phoneme set could be improved and specifically trained to analyze passwords. After which, it could be deployed as an addition to current password strength meters. It could provide users an accurate and data-driven recommendation on how usable and secure their passwords are. The existing strength meters only comment on the strength of a password and adding this feature will guarantee usable and secure passwords from the time of its creation.

The work reported in this paper is an initiative to better understand the applied usability aspects of password security. Many questions still remain in this field. We plan to continue our experiments with further research to possibly propose password policy guidelines that could maximize security and improve the usability of passwords simultaneously. Similar to the experiments performed on the merits of the password creation policies, we would also like to dwell upon the virtues of other policies, such as the frequently expiring password policy.

APPENDIX A

SCREENING SURVEY

How many workplace passwords do you have?
- 0
- 1
- 2
- 3 – 5
- 6 - 8
- 9 or more

How many of your workplace passwords are you required to change regularly? (i.e. they have an expiration policy)?
- All of my workplace passwords
- Most of my workplace passwords
- Some of my workplace passwords
- None of my workplace passwords
- Not sure

How old are you?
- 18-24 years old
- 25-34 years old
- 35-44 years old
- 45-54 years old
- 55-64 years old
- 65-74 years old
- 75 years or older
- I prefer not to answer

What is your gender?
- Male
- Female
- Other (please specify)
- I prefer not to answer

What is your race/ethnicity?
- American Indian or Alaska Native
- Asian
- Black or African American
- White/ Caucasian
- Hispanic or Latino

- Non-Hispanic
- Other
- I prefer not to answer

Which of the following best describes your highest achieved education level?

- Some High School
- High School Graduate
- Some college, no degree
- Associates degree
- Bachelor's degree
- Graduate degree (Masters, Doctorate, etc.)
- Other
- I prefer not to answer

Which of the following best describes your primary occupation?

- Administrative Support (e.g., secretary, assistant)
- Art, Writing, or Journalism (e.g., author, reporter, sculptor)
- Business, Management, or Financial (e.g., manager, accountant, banker)
- Education or Science (e.g., teacher, professor, scientist)
- Legal (e.g., lawyer, paralegal)
- Medical (e.g., doctor, nurse, dentist)
- Computer Engineering or IT Professional (e.g., programmer, IT consultant)
- Engineer in other field (e.g., civil or bio engineer)
- Service (e.g., retail clerk, server)
- Skilled Labor (e.g., electrician, plumber, carpenter)
- Unemployed
- Retired
- College student
- Graduate student
- Mechanical Turk worker
- I prefer not to answer

APPENDIX B

PASSWORD SURVEY

Users are asked to choose one password that they consider as main to keep in mind when answering these questions.

How many workplace passwords do you have?
- 0
- 1
- 2
- 3 – 5
- 6 or more

When you first created your main workplace password, which of the following methods did you use?
- Used the first letter of each word in a phrase
- Used the name of someone or something/English word
- Used a word in a language other than English
- Added/Removed numbers/symbols to the beginning or end of a word or name
- Substituted numbers/symbols for some of the letters in a word or name (e.g. '@' instead of 'a' or '3' instead of 'E')
- Used a phone number/ address/ birthday/ personal information.
- Reused a password from another account exactly
- Reused a password from another account with some modifications
- Used something else (please specify)
- I prefer not to answer

How many of your workplace passwords are you required to regularly change, i.e. they have an expiration policy?
- All of my workplace passwords
- Most of my workplace passwords
- Some of my workplace passwords
- None of my workplace passwords
- Not sure

How often are you required to change your main workplace password?
- Every week
- Every 30 days
- Every 60 days
- Every 90 days
- Every year

- Never
- Not sure
- Other (please specify)

Some organizations require their employees to change their passwords every 60 days. What do you think the impact of this policy is on security compared to organizations that do not require their employees to change their passwords at all?

- It makes it less likely that an unauthorized person will log in to my account
- It makes it more likely that an unauthorized person will log in to my account
- It doesn't impact security
- I don't know

How often do you think your workplace should require its employees to change their main workplace password?

- Every week
- Every 30 days
- Every 60 days
- Every 90 days
- Every year
- Never
- Not sure
- Other (please specify)

The last time you changed your main workplace password, what approaches did you use? (select all that apply)

- Adding a date (e.g. "kiwi" →"kiwi2018")
- Adding a sequence (e.g. "music#7"→"music#123")
- Capitalizing a character (e.g. "doghouse"→"DogHouse")
- Deleting digits/special characters (e.g. "jan16!!!" →"jan16!!")
- Incrementing a character (e.g. "password7"→"password8")
- Moving a letter, digit or special character block (e.g. "$apple30" →"30$apple")
- Substituting digits/special characters with the same character type (e.g. "cartwheel" →"c@r1whee!")
- Changing a small part of the previous password in a way not mentioned
- Creating a completely new password
- Reusing old passwords from other accounts
- Using a password generator

How often have you used your strategy to change your main workplace password when it expired?

- I only changed my password once
- A couple of times (not often)
- most of the time
- every time

- I never changed my password
- other (please specify)

When changing your workplace password because the old one expired, do you always use the same strategy?

- I use the same strategy every time
- I use slightly different strategies at different times
- I use very different strategies at different times

How similar is your main workplace password to a password you use for another account?

- My password is identical to a password I use for another account
- My password is very different from any passwords I use for other accounts
- My password is very similar (few modifications) from any passwords I use for other accounts

When I last changed my main workplace password because it had expired, my new password was:

- Much weaker
- Weaker
- About the same
- Stronger
- Much stronger
- I don't know

How many workplace passwords do you have?

- 0
- 1
- 2
- 3 – 5
- 6 - 8
- 9 or more

Frequent password expiration makes it less likely that an unauthorized person will break into my account.	Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree
I find having to change my password due to my workplace expiration policy difficult.	Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree
I find having to change my password due to my workplace expiration policy easy.	Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree

I find having to change my password due to my workplace expiration policy annoying.	Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree
I find having to change my password due to my workplace expiration policy fun	Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree
Password policies makes it less likely that an unauthorized person will break into my account.	Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree

What do you do to help yourself remember your main workplace password?
- Store it in an encrypted file
- Store it in a password manager
- Store it on a computer or device protected with another password
- Write down my password on a piece of paper
- Nothing, I memorize it

How many logins does it take for you to memorize your main workplace password?
- 1-2 logins
- 3-5 logins
- 6-10 logins
- More than 10 logins
- None, I memorize it when I create it or use a password, I already memorized

Are you either a computer security professional or a student studying computer security?
- Yes
- No

When do you get the first reminder to change your main workplace password before it expires?
- Less than a week in advance
- 1-2 weeks in advance
- 3-4 weeks in advance
- 1 month in advance
- More than 1 month in advance
- Other (please specify)

How does the reminder impact your effort in changing your main workplace password?
- I put more effort in updating my password
- I put less effort in updating my password
- It doesn't, I put the same amount of effort
- Other (please specify)

Has your main workplace password ever been accidentally leaked or otherwise compromised?

- Yes, I lost the device which had the password stored and the device was not password protected
- Yes, I lost the paper on which I wrote my password
- Yes, someone guessed it
- Yes, someone watched me type it in
- Yes, the IT infrastructure was breached
- Yes, other
- No

Are you either a computer security professional or a student studying computer security?

- Yes
- No

To keep your account secure, how important is it to store your password in a safe place (e.g., on a note hidden out of sight of other people) or not store it at all?

- 1 (Not important) – 5 (Very important)

To keep your account secure, how important is it to change your password periodically?

- 1 (Not important) – 5 (Very important)

To keep your account secure, how important is it to create a password that you do not already use somewhere else?

- 1 (Not important) – 5 (Very important)

Do you have any other comments about your password or its policies?

REFERENCES

[1] "Passphrases," *SANS Security Awareness*. [Online]. Available: http://www.sans.org/security-awareness-training/ouch-newsletter/2017/passphrases. [Accessed Apr. 5, 2019].

[2] W. Ma, J. Campbell, D. Tran and D. Kleeman, "Password Entropy and Password Quality," in *the Fourth International Conference on Network and System Security, 2010*. pp. 583-587.

[3] D. Florencio and C. Herley, "A large-scale study of web password habits," in *the 16th international conference on World Wide Web - WWW 07, 2017.* pp. 657–666.

[4] E. Von Zezschwitz, A. De Luca and H. Hussmann, "Survival of the shortest: A retrospective analysis of influencing factors on password composition," in *IFIP Conference on Human-Computer Interaction,* Eds. Berlin: Springer, September 2013. pp. 460-467.

[5] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor, "I Added '!' at the End to Make It Secure: Observing Password Creation in the Lab," in *the Symposium on Usable Privacy and Security (SOUPS), Ottawa, Canada, July 22-24, 2015.* pp. 123-140.

[6] "NIST Special Publication 800-63B," *NIST.* [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63b.html. [Accessed Feb. 05, 2019].

[7] D. Malone and K. Maher, "Investigating the distribution of password choices," in *the 21st international conference on World Wide Web, April 16-20, 2012, Lyon, France.* pp. 301-310.

[8] E. Stobert and R. Biddle, "The password life cycle: user behavior in managing passwords," in *the 10th Symposium on Usable Privacy and Security (SOUPS), 2014.* pp. 243-255.

[9] R. Yampolskiy, "Analyzing User Password Selection Behavior for Reduction of Password Space," in *the 40th Annual 2006 International Carnahan Conference on Security Technology, 2006*.

[10] A. Rao, B. Jha, and G. Kini, "Effect of grammar on security of long passwords," in *the third ACM conference on Data and application security and privacy, 2013.* pp. 317-324.

[11] Garfinkel and H.R. Lipford, “Usable security: History, themes, and challenges,” in *the Synthesis Lectures on Information Security, Privacy, and Trust, 2014.* pp.1-124.

[12] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, and J. Lopez, “Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms,” in *the IEEE Symposium on Security and Privacy, 2012.* pp. 523-537.

[13] A. A. Salah, T. Gevers, N. Sebe, and A. Vinciarelli, “Challenges of Human Behavior Understanding,” in *the Human Behavior Understanding Lecture Notes in Computer Science, 2010.* pp. 1-12.

[14] X. D. C. D. Carnavalet and M. Mannan, “From Very Weak to Very Strong: Analyzing Password-Strength Meters,” in *the Network and Distributed System Security Symposium, 2014.* pp. 23-26.

[15] N. Micallef and N.A.G. Arachchilage, “A Gamified Approach to Improve Users' Memorability of Fall-back Authentication,” in *the Fourteenth Symposium on Usable Privacy and Security (SOUPS), July 2017.*

[16] D. Wang and P. Wang, “The Emperor’s New Password Creation Policies,” in *Computer Security - ESORICS 2015 Lecture Notes in Computer Science, 2015.* pp. 456–477.

[17] M. Weir, S. Aggarwal, M. Collins, and H. Stern, “Testing metrics for password creation policies by attacking large sets of revealed passwords,” in *the 17th ACM conference on Computer and communications security - CCS 10, 2010.* pp. 162-175.

[18] C. Wang, S. T. Jan, H. Hu, D. Bossart, and G. Wang, “The Next Domino to Fall,” in *the Eighth ACM Conference on Data and Application Security and Privacy - CODASPY 18, 2018*. pp. 196-203.

[19] M.M. Devillers, “Analyzing password strength,” Radboud University, Nijmegen, Netherlands, July 2010.

[20] “Division of Information Technology,” *Cyber Security: Passphrases and Passwords.* [Online]. Available: https://it.stonybrook.edu/help/kb/cyber-security-passphrases. [Accessed Feb. 8, 2019].

[21] H. Collider, “How Secure Is My Password?,” *HowSecureIsMyPassword* [Online]. Available: https://howsecureismypassword.net. [Accessed Apr. 2, 2019].

[22] "The CMU Pronouncing Dictionary," *CMUPronouncingDictionary,* 2018. [Online]. Available: http://www.speech.cs.cmu.edu/cgi-bin/cmudict. [Accessed Apr. 19, 2019].

[23] A. Klautau, "ARPABET and the TIMIT alphabet," 2001. [Online]. Available: http://speech.ucsd.edu/aldebaro/papers. [Accessed Apr. 2, 2019]

[24] "Seatgeek/fuzzywuzzy," *GitHub,* 20-Aug-2018. [Online]. Available: https://github.com/seatgeek/fuzzywuzzy. [Accessed Feb. 02, 2019].

[25] "FuzzyWuzzy Python library," *GeeksforGeeks,* 24-Dec-2017. [Online]. Available: https://www.geeksforgeeks.org/fuzzywuzzy-python-library/. [Accessed Apr. 15, 2019].

[26] R. McMillan, "The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1^d!," *The Wall Street Journal,* 07-Aug-2017. [Online]. Available: https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118. [Accessed Apr 2, 2019].

[27] Y. Choong, M. Theofanos, and H. K. Liu, "United States Federal Employees Password Management Behaviors: A Department of Commerce case study," 2014.

[28] H. Habib, P.E. Naeini, S. Devlin, M. Oates, C. Swoopes, L. Bauer, N. Christin and L.F. Cranor, "User behaviors and attitudes under password expiration policies," in *the Fourteenth Symposium on Usable Privacy and Security (SOUPS), 2018.* pp. 13-30.

[29] R.P. Van Heerden and J.S. Vorster, "Statistical analysis of large passwords lists used to optimize brute force attacks," 2009.

[30] "Password Creation Rules," *NASA*, 24-Jun-2015. [Online]. Available: http://www.nas.nasa.gov/hecc/support/kb/password-creation-rules_270.html. [Accessed Apr. 11, 2019].

[31] R. W. Proctor, M.-C. Lien, K. P. L. Vu, E. E. Schultz, and G. Salvendy, "Improving computer security for authentication of users: Influence of proactive password restrictions," *Behavior Research Methods, Instruments, & Computers,* vol. 34, no. 2, pp. 163–169, 2002.

[32] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman, "Of passwords and people," in *the 2011 annual conference on Human factors in computing systems, 2011.* pp. 2595-2604.

[33] L. Tam, M. Glassman, and M. Vandenwauver, "The psychology of password management: a tradeoff between security and convenience," *Behaviour & Information Technology,* vol. 29, no. 3, pp. 233–244, 2010.

[34] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The Tangled Web of Password Reuse," in *2014 Network and Distributed System Security Symposium, 2014.* pp. 23-26.

[35] K. P. L. Vu, R. W. Proctor, A. Bhargav-Spantzel, B. Tai, J. Cook, and E. E. Schultz, "Improving password security and memorability to protect personal and organizational information," *International Journal of Human-Computer Studies,* vol. 65, no. 8, pp. 744–757, 2007.

[36] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password memorability and security: empirical results," *IEEE Security & Privacy Magazine,* vol. 2, no. 5, pp. 25–31, 2004.