Finding the Middle Ground: Measuring Passwords for Security and Memorability

Joshua J. Rodriguez
University of New Orleans, USA
jjrodri7@uno.edu

Minhaz F. Zibran
Idaho State University, USA
MinhazZibran@isu.edu

Farjana Z. Eishita
Idaho State University, USA
FarjanaEishita@isu.edu

***Abstract*—Passwords are a ubiquitous element of our digital age, and the need for secure passwords is indispensable. However, traditionally secure passwords tends to be very difficult to remember, leading users to frustration in having to remake them or even abandoning secure ones for the sake of memorability. On the other hand, passwords that are considered memorable have a tendency to be less secure. Despite many studies on passwords, the process of the users' perceiving password memorability is still abstract. This security and memorability trade-off brings out the need to find a middle ground leaving the research question on the ground whether finding passwords that are both memorable and secure is a possibility or not.**

In this paper, we address this very question by conducting a survey and a user-study of memorability for certain categories of popular password styles. Next, we take the most memorable of these passwords and determine their security via a bits of entropy calculation commonly used to determine a password's strength against a traditional brute force attack. Finally, we find the best performers of both memorability and security to find the middle ground of password security and memorability. Our findings present a collection of both memorable and secure styles of passwords including an infrequent but effective tactic for password remembrance.

***Index Terms*—Password, Passcode, Passphrase, Authentication, Memorability, Security, Privacy**

I. Introduction

With the enhanced aptitude of web-based platform people have increased their everyday task via internet. These frequent web-based transactions include significant amounts of personal and confidential data. To restrict unauthorized access to these large volumes of confidential data, various methods are applied such as, use of access control (e.g. file permission) after the verification of the identity of the person requested access [18] or biometric authentication. In spite of being less secure than biometric device or smart cards [13], the username-password authentication has been the most widely accepted authentication method due to its facile implementation technique [16]. Hence, the usage of passwords will retain its necessity in forthcoming generations. For many websites (e.g. social media cites) that maintain personal information, username-password is the primary method of both identification and authorization [20]. Hence, in today's digital world, passwords are so common that one would be hard pressed to find anyone who uses modern technology that does not use one.

To ensure the security of data, a strong password is the key. Oftentimes, passwords are the line between our sensitive information and an attackers nefarious intentions. The traditional course of action to generate a strong password may include larger length consisting of various combinations of alphabets, case, numbers, and special characters. The security of passwords relies on its difficulty to be learned by an attacker via different means of attacks. These often include guessing tactics such as brute-forcing, dictionary, and/or rainbow table attacks. Passwords that can withstand such attacks tend to be longer, have more random assortments of their characters, and include many types of characters. However, these passwords tend to be much more difficult for a user to remember. A password such as

```
jf%#45‘4fDsa@j*89e_3=+3Ad7$ki(}
```

is considered to be secure, but not easy to remember. If the readers are asked to spend one-minute attempting to memorize the password example above and then try to recall it after completing reading this paper, it is likely that most of the readers will find this task to be quite difficult if not impossible.

Typically the users create passwords that are easy to remember to avoid writing it down on paper or sharing it with someone. While different websites possess different criteria to create passwords to make them secure, oftentimes, users who cannot remember their passwords are forced to recreate new ones by the apps and services that they are using, making it even more difficult to remember the password. Of course, a user will want to choose a new password that is very secure, but may quickly find themselves in the same situation again the next time they must login, which can be frustrating for them. A user may consider using a password that is easier to remember, but this, to a users dismay, only helps the attacker since passwords that are easy to remember are often easy to guess. Thus, there would appear to be a trade-off. Users may choose more secure passwords, but forget them often or they may choose more memorable passwords, but be vulnerable to an attack. Naturally, a question arises from this: Are there passwords that are both memorable and secure, without lying in the extremes of security and memorability?

In this paper, we attempt to answer this question by first conducting a two-part survey and memorability test in which we ask the participants to come up with sets of new passwords given certain common password creation strategies. We then ask the participants to memorize these passwords and recall them to test the password memorability in both short- and long-term memory passes. Next, we find the most memorable

978-1-6654-8350-6/22/$31.00 ©2022 IEEE
SERA 2022, May 25-27, 2022, Las Vegas, USA

of these passwords and measure their security via calculating their bits of entropy, a tactic often used to determine a passwords strength under a traditional brute-force attack. Finally, we compile a list of the best performing passwords from these calculations and present our findings.

The rest of this paper is organized as follows: Section II describes the related work, Section III describes the overall methodology, Section IV contains the detail of conduction process of the experiment, Section V demonstrates the demographic results of the survey and the results of the memorability test along with results of the bits of entropy calculations of the best performing passwords. Section VI include a discussion of the limitations and future directions of this work. Finally, Section VII concludes this paper.

II. Related Work

There have been many studies to investigate program vulnerabilities [8], [9], [12], [15] as well as patterns and characteristics of bugs [10], [11], [17], [28] that lead to insecurity. However, the first line of defense is authentication through password or such a mechanism. But there exists a tension between memorability and security of passwords. The *memorability* and *security* of passwords have been studied in many contexts.

Vu et al. [20] explained how memorable passwords can aid people to avoid bad security practice and remember passwords easily. In this paper, the authors reviewed several factors such as generation effect, memory load, Proactive interference, Elaborative Processing and Mnemonics that amplify password memorability. The authors also provided methods to strengthen the security of passwords. However, Froget et al. mentioned most password strengthening method requires compromise with memorability; hence, proposed persuasive technology to assist users in creating stronger password [6]. Geometric shape-based password generation is proposed by Weiss and Luca with an anticipation of creating easy to remember yet complex (e.g. hence secure) passwords [21].

Research is conducted to determine the causes for difficulty in remembering multiple passwords in terms of long-term memory [27], exploring methods for improving memorability via multiple verification [23], and studying users password recall ability versus their perceptions of their recall ability to determine why users have difficulty remembering passwords [22]. Password memorability and security have also been studied together in the context of studying methods of creating memorable passwords that must also satisfy certain security conscious password criteria [20], and in studying how password policy affects recall, and the entropy, of passwords [14].

Empirical studies on improving multiple password recall is conducted by a number of researchers over time [24] [27]. In work of Zhang et al. [27], users were asked to recall their own generated passwords one week after creating them for the purpose of engaging their long-term memory, Zhang et. al. proposed that - "interference between different passwords is one of the major challenges to multiple-password recall and that interference alleviation methods can significantly improve multiple-password recall". In support of their approach, the authors conducted a lab experiment to investigate the effectiveness of list reduction method and unique identification method and demonstrated that both improved multiple-password recall performance with list reduction method being the better.

Our study applies a similar methodology, and subscribes to the same idea of Atkinson and Shiffrins Stage Memory Theory [4]. Other relevant topics include the generation effect described in [20], where the idea that user generated text is easy to remember than text given to the user to remember is presented as a support for that studys methodology for unique user password generation. This study applies a similar approach in having its users generate their own passwords. Jim Marquardson's work [14] is relevant to this study in its approach in providing password policies for the user, as well as its measurement of entropy of user generated passwords. Helkala and Svendsen presented guidelines for designing passwords with a personal factor and a relevant element associated with the website to log in, which demonstrated good memorability of strong passwords [7].

In one of the recent research, Yildirim and Mackie proposed a reliable solution by encouraging the users to create their password by using their own formula and demonstrated that their proposed methods are much more efficient than strict password policies used by many websites these days [26]. In addition, the authors claimed that through this research they have provided a low-cost guideline to solve the security and usability issues of text-based passwords. Another recent research by Alomari et al. [2] [3] present the users' perceptions of password memorability and recall. Here, using the signals received from electroencephalogram (EEG) device, the authors showed consistency between how users perceive password memorability by the least and most memorable passwords with an actual measured strength of these passwords.

This study differs from previous studies in its objective, which is to find passwords that are memorable and secure whereas previous studies objectives direct them towards determining how policies effect password creation, as in [14], providing new ways to increase memorability of passwords [23], determining why users have difficulty remembering passwords [22], determining if password restrictions lead to more secure passwords [20], and finding methods to alleviate strains on password memorization [27].

III. Methodology

The experimental procedure of the research consists of two major components: (a) data collection via survey for memorability testing and (b) analysis of memorability and security of passwords. Two major components of the survey included the memory test survey and the demographic data collection. Section IV-A contains the detail of memory survey followed a description of the participants' demography in Section IV-B.

This survey is conducted in two parts. The first part includes questionnaires to analyze short-term memory and the second part collects data to analyze the long-term memory of the participants. Previous works on passwords typically discussed password security and improvements. Some research explored password usage and memory [25], or even more akin to this study password security and memorability [5]. However, while these works discussed memory and conducted memorability surveys, none of them accounted for different modal models of memory. The original literature for modal models of memory [4] describes memories as passing through short-term and long-term stores. These short-term memories may last only a few seconds to minutes, and long-term memories can last for years or a lifetime. Passwords, as memories, may be considered to pass through these stores in this modal model of memory. In this study, tests for both short-term and long-term memories are included.

There are three phases in the memory test. In each phase, four different kinds of password creation criteria were presented as coded and defined below:

Phase-1:

- PW-8L: Create a password with 8 random characters using only lowercase
- PW-8LNS: Create a password with 8 random characters using lowercase letters, at least one symbol, and at least one number (must be different from the above)
- PW-12L: Create a password with 12 random characters using only lowercase
- PW-12LNS: Create a password with 8 random characters using lowercase letters, at least one symbol, and at least one number (must be different from the above)

Phase-2:

- PP-3: Create a passphrase with 3 random words that are not separated by spaces
- PP-3NSC: Create a passphrase with 3 random words that are separated by numbers, symbols, or random characters (MUST be different from the above)
- PP-5: Create a passphrase with 5 random words that are not separated by spaces
- PP-5NSC: Create a passphrase with 5 random words that are separated by numbers, symbols, or random characters (must be different from the above)

Phase-3:

- PPL-5: Create a passphrase with a short sentence (at least 5 words) from any random piece of literature (i.e., novel, poem, play) that has no spaces between words
- PPL-5NSC: Create a passphrase with a short sentence (at least 5 words) from any random piece of literature that have numbers, symbols, or random characters between each word (must be different from the above)
- PPL-7: Create a passphrase with a long sentence (at least 7 words) from any random piece of literature that has no spaces between words
- PPL-7NSC: Create a passphrase with a long sentence (at least 7 words) from any random piece of literature that have numbers, symbols, or random characters between each word (must be different from the above)

IV. Experiment

A. Memory Test Survey

The participants partook in a memory test consist of three phases as mentioned in section III. After each phase, the participants were given four minutes to memorize these passwords with a tactic of their choice. Then they were asked to step away from the test for five minutes before reentering them. Since this five minute span is just on the edge of the short-term memory pass as described in the modal models of memory, we consider this to be an apt test of short-term memory of these passwords.

After completion of the first part of the survey, the participants were told that they will be contacted again at a random time within the next seven days to participate in the long-term memory test in which they will need to recall and write these passwords again. Since one to seven days is well out of the short-term memory pass and into the long-term memory pass, we consider this to be an apt test of long-term memory of these passwords.

B. Capturing Demography

The survey was conducted with 36 individuals of whom 13 responded to the first part and nine of those 13 responded to the second part. There were six female participants and seven male participants in total with ages ranging from 22-61 with 28.5% being over 30 years old. Occupations ranged from Students to IT technician to Legal Secretaries to Restaurant Managers to Photographers to Civil Engineers to Ophthalmic Technicians. The questionnaire provided to collect the demographic information is listed in Table I.

TABLE I
Questionnaire for Capturing the Demographic Information about the Survey Participants

- What is your age?
- What is your profession?
- What is your level of education?
- How would you describe your computer literacy?

("Very Literate" may describe someone who has an in depth understanding of how a computer works at the software and hardware level, whereas "Very Illiterate" may describe someone who has great difficulty navigating a desktop.)

- How often do you use passwords?
- How many different passwords do you currently use?
- Do you believe that your passwords are secure?
- Do you have difficulty remembering new passwords when asked by a system to create a new one?
- Do you keep a physical copy of your passwords?
- If so, do you keep a copy of all of them or just some of them?

V. Findings

A. Demography

A total of 46.2% of the participants reported to have earned a bachelors degree, 23.1% reported a high school diploma or associates degree and 7.7% a graduates degree. When asked about their computer literacy 46.2% reported themselves as somewhat literate, 38.5% as literate, and 15.4% as very literate. When asked about the frequency of their password usage, all participants responded that they used them multiple times per day. Three of the 13 participants mentioned that they used 15 or more passwords in total, while the rest described using less than 10 with 5 of them stating that they used 5 or more. A majority (61.5%) of the participants reported having difficulty remembering new passwords.

TABLE II
EXAMPLES OF PARTICIPANT-CREATED PASSWORDS ACCORDING TO THE GIVEN CRITERIA FOR PHASE-1

PW-8L	PW-8LNS	PW-12L	PW-12LNS
nlegsamo	enobmah_1	dettbailcate	olliejulcris_1
mnwensmg	mnw1319$	hntjcwdnblnb	qaz34$plm131
swparner	l0tr@m3!	swparnerflri	f0tr2tr0tk@3
Asgscdcs	krlrma7!	Sscspaoophbp	Kmdmmmbmmm6!
Jeajjajy	Jeajja@1	Jeajjajymdss	Jeajjajymd@!
polkmnwq	wqsaxzpo1!	qwaszxopklnm	opklnmqwaszx1!

B. Memorability Test

1) Short-Term Memorability Test Results: An example of the outcomes of the memorability test for part 1 of the survey is depicted in Table II, III, and IV. This shows the type of passwords entered into the tests. In Table V, the results of the short-term memory test are shown that demonstrates how many passwords for each given criterion were incorrectly entered. An incorrect entry is considered incorrect in these tests if any single character does not match the initially created password. Correctness was determined manually for all memory tests.

As can be seen in Table V, passphrases tend to perform the best in terms of memorability. Interestingly, some participants chose to create rhymed sequences of words for their passphrases such as DrownBrownFrownClown. In our study, we found that every time this method is employed, participants were always able to remember them with 100% accuracy.

2) Long-Term Memorability Test Results: The results of the long-term memory test were determined via correctness. In Table VI, each password criteria is given showing how many of the 9 participants successfully entered the passwords after 1-7 days. Passphrases from literature that are 5 words long with no symbols, numbers, or characters in-between words scored almost perfectly in this phase. Surprisingly, 12 random character long passwords did second best.

C. Password Security

The best performers were chosen from the memorability tests, and were run through a simplified bits of entropy calculation based on the work of Shannon [19] determine their baseline strength. The formula used is as such:

$$\text{Bits of Entropy} = Log_2(p^L) \tag{1}$$

where p is the symbol pool and L is the length in characters of the password.

Greater than or equal to 70 bits of entropy was considered to be sufficiently secure since a password with 70 bits of entropy might take 37 years at least to crack using one trillion guesses per second. This was derived by the following formula:

$$\text{Years to Crack} = \frac{2^b/G}{S} \tag{2}$$

where b is bits of entropy, G is guesses per second, and S is seconds per year.

The best performers here were determined by having at most three incorrect guesses on the short-term memory test and at least four correct guesses on the long-term memory test. The results are as follows.

D. PW-12L

Passwords with *12 random characters only* were guessed incorrectly in the short-term test three times, and were guessed correctly in the long-term test five times.

In total, *12 lowercase characters only* creates 56.4 bits of entropy. However, because of the random choice of characters, dictionary attacks are not possible. If an attacker brute-forced this password with 10,000-1,000,000 guesses per second, this may take hundreds of days to a couple of days. Any higher guesses per second may take hours to minutes to crack, making this type of password less secure than needed despite its memorability.

E. PP-3

Passphrases with *three random words only* were never guessed incorrectly in the short-term, and were guessed correctly in the long-term test four times.

The *three 4-letter lowercase words only* creates 56.4 bits of entropy, but *three 5-letter lowercase words* can create 70.5 bits of entropy. If an attacker brute-forced this three 5-letter word password with 10,000-1,000,000 guesses per second, this may take billions to millions of years to crack, making this type of password fairly secure if the proper choice of letter words is used. These may also be vulnerable to dictionary style attacks.

F. PP-5

Passphrases with *five random words only* were guessed incorrectly in the short-term only once, and were guessed correctly in the long-term test four times.

The *five 3-letter lowercase words* creates 70.5 bits of entropy, but *five 4-letter lowercase words* can create 94 bits of entropy. If an attacker brute-forced this five 4-letter word password with 10,000-1,000,000 guesses per second, this may take quadrillions to hundreds of billions of years to crack, making this type of password secure if the proper choice of letter words is used. However, these may be vulnerable to dictionary style attacks.

G. PPL-5

Passphrases from literature with *five random words only* were guessed incorrectly in the short-term test only twice, and were guessed correctly in the long-term test eight times.

Again, *five 3-letter lowercase words* creates 70.5 bits of entropy, but *five 4-letter lowercase words* can create 94 bits of entropy. If an attacker brute-forced this five 4-letter word password with 10,000-1,000,000 guesses per second, this may

TABLE III
EXAMPLES OF PASSWORDS ACCORDING TO THE GIVEN CRITERIA FOR PHASE-2

PP-3	PP-3NSC	PP-5	PP-5NSC
Catsanddogs	Me4is5tired	willforgettheseforsure	Kinda!want6tacos&beer?you
leanweenpeen	skake_balcony_dead	onoffleftrightdown	lights_camera_action_rolling_cut
Earspoonwatch	Pizza0chapelle8candle	Sockcardspumpkinlightpaint	Office1broomstick2book3turkey4coffee
fakesnakelake	think1stink2pink	drownbrownfrownclown	free;pre-knee/tree
Monkeyapricotgelato	Tulip90November@>Hollow	FranceGigawattArteryJamesOnion	Police535CommaxcxCoffin_EuropewdghParticular

TABLE IV
EXAMPLES OF PARTICIPANT-CREATED PASSWORDS ACCORDING TO THE GIVEN CRITERIA FOR PHASE-3

PPL-5	PPL-5NSC
ToBeOrNotTo	Something!Wicked?This$Way@Comes
ifmyfearshaveeyes	out_of_some_subway_scuttle
tobeornottobe	those-who/dont:believe;in(magic)wont$find&it
werenotgonnatakeit	i!saw)her1standing0there
Notmenothermoineyou	After1all2this3time!always
thoushaltnotcovetthyneighborsgoods	the*time*is*just*before*dawn

TABLE V
MEASURES OF INCORRECT PASSWORD ATTEMPTS FOR 13 PARTICIPANTS

Criteria	Incorrect	Criteria	Incorrect
PW-8L	2	PW-8LNS	4
PW-12L	3	PW-12LNS	4
PP-3	0	PP-3NSC	1
PP-5	1	PP-5NSC	2
PPL-5	2	PPL-5NSC	2
PPL-7	2	PPL-7NSC	2

TABLE VI
MEASURES OF CORRECT PASSWORD ATTEMPTS FOR 9 PARTICIPANTS

Criteria	Correct	Criteria	Correct
PW-8L	4	PW-8LNS	2
PW-12L	5	PW-12LNS	2
PP-3	4	PP-3NSC	3
PP-5	4	PP-5NSC	3
PPL-5	8	PPL-5NSC	1
PPL-7	4	PPL-7NSC	4

take quadrillions to hundreds of billions of years to crack, making this type of password secure if the proper choice of letter words is used. However, these may be vulnerable to dictionary style attacks.

H. PPL-7

Passphrases from literature with *seven random words only* were guessed incorrectly in the short-term test only twice, and were guessed correctly in the long-term test four times.

The *seven 3-letter lowercase words* creates 98.7 bits of entropy, but *seven 4-letter lowercase words* can create 131.6 bits of entropy. If an attacker brute-forced this seven 4-letter word password with 10,000-1,000,000 guesses per second, this may take a near infinite number of years to crack, making this type of password very secure if the proper choice of letter words is used. Similar to PPL-5, these may be vulnerable to dictionary style attacks.

I. PPL-7NSC

Passphrases from literature with *seven random words separated by numbers, symbols, and random characters* were guessed incorrectly in the short-term test only twice, and were guessed correctly in the long-term test four times.

The *seven 3-letter lowercase words* separated by numbers, symbols, and random characters creates 127.8 bits of entropy, but *seven 4-letter lowercase words* separated by numbers, symbols, and random characters can create 170.4 bits of entropy! If an attacker brute-forced this seven 4-letter word password with 10,000-1,000,000 guesses per second, this may take a near infinite number of years to crack, making this type of password very secure if the proper choice of letter words is used. Moreover, these passwords are not vulnerable to dictionary style attacks!

VI. DISCUSSION

In this study, it was found that certain password styles perform better in terms of memorability and security. For instance, PP-3 performs best in short term memorability, but only begins to perform well in security when higher lettered words are used. However, such a password may be found easily if an attacker uses a dictionary attack. Given this, the more uncommon the words, the harder it will be to find.

PPL-5 was the best performing in long term memorability, and did well in security even if small 3-letter words were used. However, such a password may be found easily if an attacker has some list of popular phrases/sentences from literature. Given this, the more obscure the literature, the better. Bible quotes and Shakespeare are probably not secure enough.

PPL-7NSC was the best performing in security, and performed well in memorability. While an attacker may find this password easily if they had some list of popular phrases/sentences from literature, the added numbers and symbols may break this. A dictionary attack may still be effective, but again, the added letters and symbols make this type of attack much more difficult. This type of password has the best security bang for your memorability bucks!

We also found that passphrases that contained rhymed words were highly memorable to the participants in the study and used often by them. Given the novelty of this discovery, we believe that this may warrant future work to properly decern the security of such passwords.

It is in our knowledge that the study was conducted with a small pool of participants. A large scale user experiment including various ranges of people is in the pipeline. We intend to investigate the outcome based on age as well as level of security literacy. In addition, the real-world password attack will be in consideration. Bits of entropy calculations can only take us so far, and in this study, it was used as a simple baseline to determine security against a traditional brute-force attack. Future work may consider creating mock attacks to test real-world attack strategies on these passwords.

To ensure privacy, users need to adopt generating effective passwords in terms of security and memorability. Typically, the passwords that are easy to remember tend to be vulnerable and less secure. In attempt of ensuring security, people compose passwords that are difficult to remember. Moreover, various websites restrict the characters and symbols, which leads a person to taking on the burden of maintaining multiple passwords. To balance the security and memorability the user adopts ill-protected habits such as writing the password or sharing it with someone. In addition, if the user forgets a password and is in need of creating a new one, some websites restrict certain reuse of previously used passwords.

VII. Conclusion

A press release conducted by RSA security showed that 30% of the total survey participants manage 6–12 passwords and 28% of them expressed that they need to maintain 13 passwords [1] [20]. With these restrictions, while maintaining passwords, it is difficult for users to remember their passwords for specific sites. Hence, analyzing the trade-off between password strength in terms of security and memorability is essential. In this paper, we confront the trade-of between password security and memorability by conducting a two-part survey and memorability test followed by an entropy analysis to identify the correlation between the most memorable passwords (in both short-term and long-term memory) and their security. Finally, a list of best performing passwords in terms of security and memorability is conferred.

References

[1] RSA cybersecurity and digital risk management solutions, Jan 1982.

[2] R. Alomari, M. Martin, S. MacDonald, C. Bellman, R. Liscano, and A. Maraj. What your brain says about your password: Using brain-computer interfaces to predict password memorability. In *15th Annual Conference on Privacy, Security and Trust (PST)*, pages 127–136, 2017.

[3] R. Alomari, M. Martin, S. MacDonald, A. Maraj, R. Liscano, and C. Bellman. Inside out-a study of users' perceptions of password memorability and recall. *Journal of Information Security and Applications*, 47:223–234, 2019.

[4] R. Atkinson and R. Shiffrin. Human memory: A proposed system and its control processes. volume 2 of *Psychology of Learning and Motivation*, pages 89–195. Academic Press, 1968.

[5] A. Brown, E. Bracken, S. Zoccoli, and K. Douglas. Generating and remembering passwords. *Applied Cognitive Psychology*, 18:641 – 651, 09 2004.

[6] A. Forget and R. Biddle. Memorability of persuasive passwords. In *CHI'08 extended abstracts on Human factors in computing systems*, pages 3759–3764. 2008.

[7] K. Helkala and N. Svendsen. The security and memorability of passwords generated by using an association element and a personal factor. In Peeter Laud, editor, *Information Security Technology for Applications*, pages 114–130. Springer Berlin Heidelberg, 2012.

[8] M. Islam and M. Zibran. A comparative study on vulnerabilities in categories of clones and non-cloned code. In *10th IEEE Intl. Workshop on Software Clones*, pages 8–14, 2016.

[9] M. Islam and M. Zibran. On the characteristics of buggy code clones: A code quality perspective. In *12th IEEE Intl. Workshop on Software Clones*, pages 23 – 29, 2018.

[10] M. Islam and M. Zibran. How bugs are fixed: Exposing bug-fix patterns with edits and nesting levels. In *35th ACM/SIGAPP Symposium on Applied Computing*, pages 1523–1531, 2020.

[11] M. Islam and M. Zibran. What changes in where? an empirical study of bug-fixing change patterns. *ACM Applied Computing Review*, 20(4):18–34, 2021.

[12] M. Islam, M. Zibran, and A. Nagpal. Security vulnerabilities in categories of clones and non-cloned code: An empirical study. In *11th ACM/IEEE Intl. Symposium on Empirical Software Engineering and Measurement*, pages 20–29, 2017.

[13] B. Ives, K. Walsh, and H. Schneider. The domino effect of password reuse. *Communications of the ACM*, 47(4):75–78, 2004.

[14] J. Marquardson. Password policy effects on entropy and recall: Research in progress. volume 6, pages 4824–4832, 01 2012.

[15] D. Murphy, M. Zibran, and F. Eishita. Plugins to detect vulnerable plugins: An empirical assessment of the security scanner plugins for wordpress. In *Intl. Conference on Software Engineering, Management and Applications*, pages 39–44, 2021.

[16] B. Pinkas and T. Sander. Securing passwords against dictionary attacks. In *9th ACM Conference on Computer and Communications Security*, pages 161–170, 2002.

[17] A. Rajbhandari, M. Zibran, and F. Eishita. Security versus performance bugs: How bugs are handled in the chromium project. In *Intl. Conference on Software Engineering, Management and Applications*, pages 1–7 (to appear), 2022.

[18] E. Schultz, R. Proctor, M. Lien, and G. Salvendy. Usability and security an appraisal of usability issues in information security methods. *Computers & Security*, 20(7):620–634, 2001.

[19] C. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423, 1948.

[20] K. Vu, R. Proctor, A. Bhargav-Spantzel, B. Tai, J. Cook, and E. Schultz. Improving password security and memorability to protect personal and organizational information. *Intl. Journal of Human-Computer Studies*, 65(8):744–757, 2007.

[21] R. Weiss and A. De Luca. Passshapes: utilizing stroke based authentication to increase password memorability. In *5th Nordic conference on Human-computer interaction: building bridges*, pages 383–392, 2008.

[22] N. Woods and M. Siponen. Too many passwords? how understanding our memory can increase password memorability. *Intl. Journal of Human-Computer Studies*, 111:36–48, 2018.

[23] N. Woods and M. Siponen. Improving password memorability, while not inconveniencing the user. *Intl. Journal of Human-Computer Studies*, 128:61–71, 2019.

[24] J. Yan, A. Blackwell, R. Anderson, and A. Grant. Password memorability and security: Empirical results. *IEEE Security & privacy*, 2(5):25–31, 2004.

[25] J. Yan, A. Blackwell, R. Anderson, and A. Grant. Password memorability and security: Empirical results. *IEEE Security & Privacy*, 2(05):25–31, 2004.

[26] M. Yıldırım and I. Mackie. Encouraging users to improve password security and memorability. *Intl. Journal of Information Security*, 18(6):741–759, 2019.

[27] J. Zhang, X. Luo, S. Akkaladevi, and J. Ziegelmayer. Improving multiple-password recall: an empirical study. *European Journal of Information Systems*, 18(2):165–176, 2009.

[28] M. Zibran. On the effectiveness of labeled latent dirichlet allocation in automatic bug-report categorization. In *38th Intl. Conference on Software Engineering (ICSE) Companion*, pages 713–715. ACM, 2016.