Passwords and User Behavior

Tehreem Hussain*, Kiran Atta, N. Z. Bawany, Tehreem Qamar
Department of Computer Science and IT, Jinnah University for Women, Karachi, Pakistan.

* Corresponding author. Tel.: +923353260430; email: tehreemh1993@gmail.com
Manuscript submitted June 13, 2017; accepted August 10, 2017.
doi: 10.17706/jcp.13.6.692-704

Abstract: Text based passwords are commonly used for authentication in computing environment. Although passwords are considered as the initial line of protection for users but they remain easy to compromise. To improve the security of systems, various password composition polices are adopted. These policies ensure that users are made to choose strong passwords that help prevent online breaches and data leaks. However, it also make passwords difficult to memorize and recall, decreasing the overall usability. In this study we investigated the usability of password policies and users' perceptions of password security. We conducted a user study based on experimental evaluation and online survey. During the experimental evaluation users were asked to set their passwords using four different password polices. We used multiple experiment set-ups and scenarios to create real life situations. The result highlights the key difficulties faced by the users in recalling complex passwords and their inclination towards setting easy-to-guess passwords. We also studied the impact of age and domain knowledge on choosing passwords. The analysis shows that complex password polices are annoying for users and it takes more time to create such passwords. Similarly, to increase the memorability of passwords majority of users choose family member names and common dictionary words in their passwords. Using same passwords for the multiple accounts was also a common practice noticed during the study. We also evaluated the resistance of passwords created by the users against popular attacks using various password cracking tools.

Key words: Password usability, password security, password policies, password behavior.

1. Introduction

A good password comprises alphanumeric characters, digits, small and capital letters and should not consist of words from dictionary. Passwords should not be written down in an easily accessible place, especially next to login area [14]. It is critical for a user to pick strong passwords that are different for each of important accounts. Some users use same passwords for multiple accounts. Using same passwords for multiple accounts is like using same key to unlock your home, car and office. If the intruder gets entrance to one so he gets the entrance for all. If passwords are simple and easy to remember then they can be easily cracked. Strong passwords, which include the combination of characters, numbers and alphanumeric characters are difficult to crack but they cannot be easily recalled by the user, which decreases the usability of passwords. While creating various accounts, users often set passwords which are memorable and therefore are easy to guess thereby decreasing the security of their accounts. In 2016, 32 million Twitter Accounts and 360 million MySpace account passwords were hacked and their passwords were leaked [1], [2]. Most of the password leaked comprised of dictionary word, name and simple numbers For example "12345" appears 120,417 times and word "password" appeared 17,471 times [3]. In 2016, Mark Zuckerberg got several of his non-Facebook social media accounts hacked including Twitter. This happened because he

was using "dadada" as his password on multiple accounts [3].

To prevent users from picking passwords that can easily be cracked by hacker, system administrators adopt password-composition policies (e.g., requiring passwords to contain symbols and numbers)[4]. Complex password policies not only affect the composition of password but also user behaviour. For instance, if the password policy forces user to create a complex password that user cannot remember the user is expected to write down the password. Also, users may employ same password for their various accounts so that they have to remember only one password. Users are not aware that adapting such behaviour tends to decrease the account security.

This study is a substantial step forward in understanding the impact of various factors on password created by users. These factors include, age, computer science knowledge, gender, password polices etc. We aim to study user behavior and sentiments regarding their passwords. To understand the relationship between usability and security of passwords we define eight hypotheses. These hypotheses were evaluated by conducting a user study based on lab experiment and an online survey. Around 300 participants were recruited for this study. Multiple experiment set-ups and scenarios were used to create real life situations for users. Following are the interesting observations of the study:

- Many users prefer same passwords for multiple accounts to reduce the burden of remembering multiple passwords. Such users ignores the threat that their all accounts can be compromised. Usability is preferred over security.
- The systems which enforces complex password policies annoys user.
- Time to create a password increases with the complexity of password policy.
- When forced to use a complex passwords, users defines a complex password once and uses the same password with minor modification for multiple accounts. (For e.g. changing a single character only)
- Majority of users use family member names, personal information, and dictionary words in their passwords. Such users are not aware of the vulnerability of these passwords.
- Memorability and usability of a password is typically preferred over security by the users.
- Users are not aware of the fact that simple passwords can be easily cracked leading to hacking of accounts.
- Young users are more concerned about the security of their accounts therefore they prefer to create complex passwords.

The rest of the paper is organized as follows. Section 2 discusses the related work. Section 3 elaborates the hypotheses, experiments and survey on which this study is based. Results and discussions is presented in Section 4 and Section 5 respectively. Section 6 concludes the paper.

2. Related Work

Users often create passwords that are memorable which makes them vulnerable as they are easy to guess. Many studies have been conducted to evaluate the impact of password creation policies and password meters on users password creation behavior. Table 1 summarizes few such studies that had been conducted recently.

To study the behaviour of using same passwords across multiple websites a study was conducted in [5]. The survey presents responses which measures actual online behaviour gathered from 134 participants over the course of six weeks. Results show that users frequently re-use passwords particularly that are complex. Their findings suggest that users manage the challenge of remembering many passwords for various sites by choosing a one complex password. Users memorize one password and then use the same passwords for all their accounts. The study in [6] have explored how an attacker guesses user passwords. They estimate that 43-51% of users reuse password for different sites. They also found that users do slight changes in their passwords. They have also have developed password guessing algorithms that was able to guess 30% modified password with in 100 attempts [6].

Researchers have been actively involved in studying the impact of password meters and password

composition policies on security and usability of passwords. Password meters effect users' behaviour and security and help users create strong passwords. A two-part study was conducted online using Amazon's Mechanical Turk service, with 5,000 participants. In the first part various conditions were assigned randomly to each user. Then, they were asked to create a password, complete an online survey, and then enter the password. In second part, user were asked to return to their website, login using their password, and complete a second survey. They found that comprenhensive8 policy was most difficult among all policies. Because only about 17.7% of the users were able to set their passwords on first attempt [4]. The effect of password composition policies is studied in [7]. The study evaluated the password composition policies based on creation time, memorability and security. The study concluded that the passwords created using complicated password policies are more secure but less memorable [7]. A survey was designed to study the password handling, password composition, password storage, password reuse, and user sentiments of new password requirements in [8]. Around 470 students, faculty, and staff were recruited for the study. These participants had to change their passwords to comply with the new password policy requirements. They concluded that although users understood that security of their accounts have increased but they were not happy with complex passwords. To study the impact of password meters on password creation, [9] conducted a survey involving more than 2000 participants. Various password policies and password meters were used to evaluate the strength and usability of passwords. An online study was conducted to test users' perceptions of password strength and memorability, as well as their understanding of attacker models in [10]. R. Shay *et al.* [11] conducted two online studies to examine password policies with over 20,000 participants, from Amazon Mechanical Turk and collected both usability and password strength data. Their findings indicate that password strength and password usability are not necessarily inversely correlated: policies that lead to stronger passwords do not always reduce usability.

In this research paper we have studied users' behaviour and their sentiments regarding passwords by setting up experiments and survey. We evaluated the impact of various password composition polices on password creation. We also analysed the usability and vulnerability of passwords created using various policies that includes Basic8, Basic 16, Comprehensive8, and Dictionary 8.

Table 1. Summary of Various Studies Conducted to Understand Passwords and User Behavior

User Behaviour	Description
Password reuse [7], [2], [15]	Reusing same password across multiple website decrease password security. Users re-use same password with little modification on different account. User gives preference to password usability rather than security.
Password memorability and security[12]	Users tend to decrease their password security for the sake of password memorability. Difficult Password composition policy make user write down their password.
Password composition policies [11], [4], [8]	Password composition policies enable user to create strong and secure password. Password policy restrict user to create password under some criteria and pattern to make their password secure. Most commonly used password policy is comphrehensive8 which constrain user to use Digits, Symbols, Uppercase, lowercase letter.
Password strength meter[9], [13]	Password strength meter help in the process of setting up a strong password through progress meter. Different password meter have different effect on user behaviour while creating password. Visual appearance of password strength meter play a vital role in setting up a password.

3. Methodology

We conducted two experiments and an online survey to evaluate our hypotheses. The first experiment is conducted to analyse the password creation behaviour of user on various websites. In the next experiment we evaluate the memorability and usability of passwords. User is required to create a password, fill in a survey form and has to login using this password after three days. We employed four different password policies to create strong passwords. These policies are Basic8, Basic16, Dictionary8 and Comprehensive16.

3.1. Hypotheses

1. User reuse same password for multiple accounts with little modification.
2. Only few users are aware of the fact that using same password decreases the security.
3. Computer graduates / computer literate user know the fact that reusing same password decrease password security but still they reuse the same password.
4. Mostly users use dictionary word, their personal information, phrases and common names as their password.
5. Complex passwords created using password policies are difficult to memorize and recall
6. The policies which are more complicated take more time by user to create password.
7. Different age groups have different type of passwords.
8. Password meter help user to create better password.

3.2. Study and Experiments Overview

We recruited 240 responders for our online survey through Social Networking websites. For our experiment set we recruited 121 participants. Around 50% the participants were undergraduate student of Computer Science. We developed four websites for executing experiments. Each website presented scenarios and users were asked to create passwords. They were later asked to sign in again using the passwords that they created.

3.1.1. Experiment I

Scenario 1: Users were asked to create an account for ecommerce site. They were asked to select a product and follow the instructions to make an online purchase from the website we created for experiment.

Scenario 2: Users were asked to create an account for online banking. They were asked to transfer money to another account using the website we created for experiment.

Scenario 3: Users were asked to create an email account using the website we created for experiment.

3.1.2. Experiment II

Experiment II is a two part study regarding password policies. First users were asked to create an account for a social networking site. In order to create account, users were asked to take all the steps that they would usually take when creating a password. Users were strictly told not to write down their password anywhere. After creating password a quick 1 minute survey was conduct regarding their experience about password they create using one of the four policies, that is Basic8, Basic16, Dictionary8 and Comprehensive8 [4]. Basic8 policy requires password to be of at least 8 characters whereas Basic16 policy requires at least 16 characters. In contrast, Dictionary8 policy not only imposes the restriction of at least 8 characters but also requires that password is not a dictionary word. Comprehensive8 is a most stringent policy, the requires that password must include digits, symbols, uppercase and lowercase character and should contain a dictionary word. In second part of experiment, after 3 days of creating password users were again recruited. They were asked to recall their passwords and login to their account. Users were allowed 5 attempts only.

3.3. Measuring Password Strength

To evaluate the strength of passwords created using four policies we tried various methods to crack the passwords. This study contains different attack to crack the password. Different metric are used to estimate the strength of password. We used Fireforce plug-in, which works on Mozilla Firefox browsers to launch

dictionary attack and brute force attack. Password guessing algorithm is used to perform guessing attack on password hashes. To check the strength of password Hash killer and crack station was used.

3.4. Survey Design

This section discusses the design and rationale of survey. We designed an online survey that would bring honest and truthful information about passwords from our survey responders. Responders would normally take less than 5 minute to complete the survey. The questionnaire included demographic information such as age, gender and field of study. Demographics of users is shown in Table 2, Table 3. To understand the password behaviour, we included questions such as type of password preferred, frequency of changing passwords, using forget password option, sharing passwords etc. Survey also included questions to probe the usability, memorability and security preferences.

Table 2. User Divided According to Age

Age groups	No. of users	Percentage of users
Between 15 to 45	218	89%
Above 45	15	6%
Other	12	5%

Table 3. User Divided according to Gender

Gender	No. of users	Percentage of users
Male	112	46%
Female	131	53%
Don't want to answer	2	1%

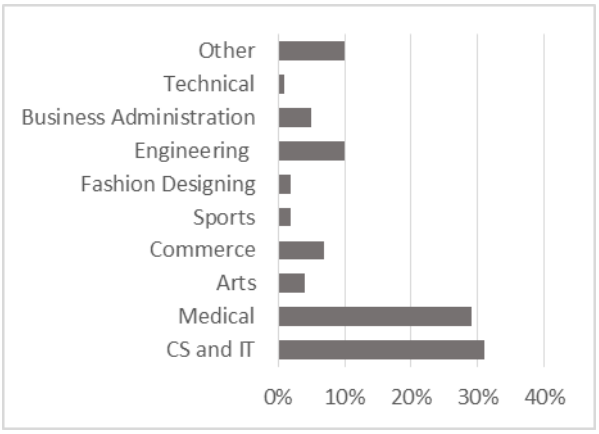

Fig. 1. Fields/profession of user.

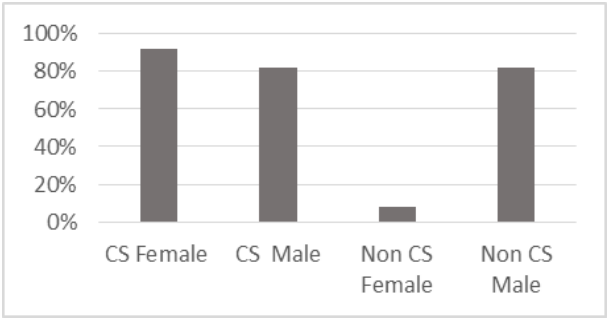

Fig. 2. Computer science and Non CS male and female.

In online survey ratio of female respondent was a bit high than male respondent. 53% were female and 46% were male. The 89% of respondent were 14-45 group of age, 6% were from above 45 groups. 14–50 group of age respondent were high in percentage than above 45 group of age. The majority of participants belonged to medical and computer science fields as depicted in Fig. 1.

4. Password Results

The table shows the average account creation time, average login time and average number of tries to login. We observed that the users took long to recall their passwords as they were logging in after 2-3 days for the first time.

Table 4. Password Creation and Login Time for Different Password Policies

Policy	Number of users	Avg. time to create an account (sec)	Avg. time to login (sec)	Average Login Tries
Basic8	26	8.02	27.08	1.25
Basic16	25	41.3	32.818	1.523
Comp8	30	29	64	2.133
Dict8	40	28.45	26.17	1.73

Table 5. User Experience while Creating Password

Questions	Basic16	Basic8	Comp8	Dic8
Were password policies helpful for you?	Yes:60% No: 40%	Yes:66.7% No: 33.3%	Yes:73% No:27%	Yes:76% No:24%
Are you concerned about your password security?	Yes:76% No: 24%	Yes:85.2% No: 14.2%	Yes:97% No:3%	Yes:92% No:8%
Will you use this policy in future to make your password secure?	Yes:48% No: 52%	Yes:66.7% No: 33.3%	Yes:40% No: 60%	Yes:88% No:12%
Are you satisfied with the password you have entered?	Yes:56% No: 44%	Yes:85.8% No: 14.2%	Yes:74% No: 26%	Yes:84% No:16%
Did you feel any difficulty while setting your password?	Yes:36% No: 64%	Yes: 3.7% No: 96.3%	Yes:77% No:23%	Yes:52% No:48%

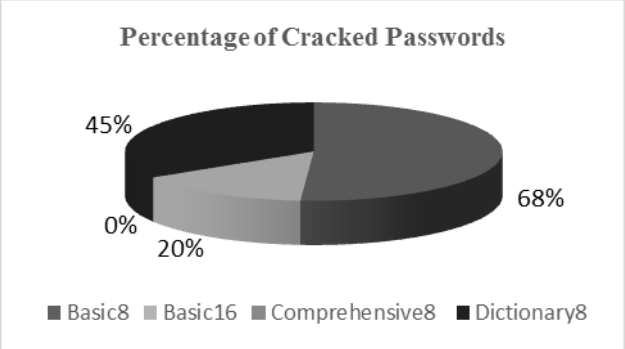

Fig. 3. Percentage of password crack.

To evaluate the user experience regarding password creation using policies we asked users to fill in the

post task questionnaire. The results are summarized in Table 5. All the password policies were tested and we found that Comphrehensive8 is more secure but less usable. Baisc8 was more usable but less secure, 68% of it was easily cracked. In Basic16, 20% passwords hashes were cracked and in dictionary8, 46% passwords hashes were cracked, in dictionary8 the hashes which were cracked were those who have dictionary words, but those hashes did not crack that have non-dictionary words. Therefore, we can conclude Dictionary8 policy is more secure and usable.

5. Analysis and Discussion

This section evaluates the hypotheses we presented in Section 3. We evaluated the hypotheses on the basis of experiments and survey.

Argument 1: Users reuse same passwords for multiple accounts with little modification

Users give more preferences to usability rather than security of their password. They rephrase their password and use it on multiple websites. Internet users probably use more than 10 websites on average which require passwords. Users tend to reuse the same password for multiple websites.

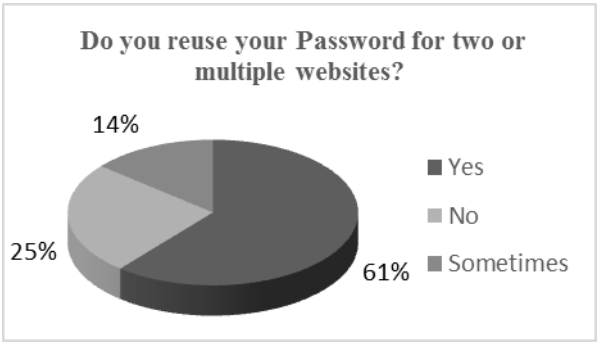

Fig. 4. Percentage of survey respondent who reuse password.

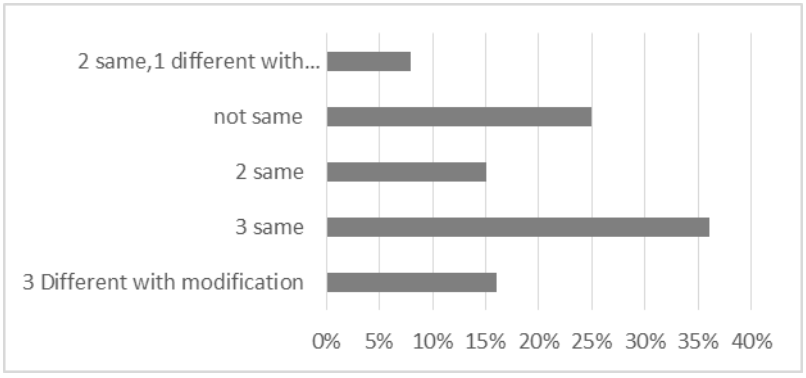

Fig. 5. Experiment users who reuse passwords.

To verify our assumption we asked our respondent whether they reuse the same password for multiple websites, 61% of the respondents said 'Yes', 25% said 'No' and 14% said 'Sometimes' as show in Fig. 4. To further validate our theory, we analyse our data collected from experiment 1 in which user were given different scenario and they were told to create an account on three websites; they were asked to create accounts like they do in reality. After analysing all the passwords we found that 36 % of users used the same password for all three accounts. 15% of the users reused the same password for two accounts and 16 % of them reused the passwords with minor modification in all three accounts as shown in Fig. 5. These results prove our hypothesis is true.

Argument 2: Only few users are aware of the fact that using the same password decreases security

All users are concerned about their password security. However, they are unaware of the fact that reusing the same passwords on multiple websites decreases their account security.

We asked our responders in online survey that "Do you know reusing same passwords for multiple website decrease your account security?" 45% said 'No' and 55% said 'Yes' as shown in Fig. 6. The responders who were unaware of password security were 15% from Medical, 5% from Engineering,, 3% from Commerce,1% from Arts,3% from Computer Science and IT 3% from Business Administrator and 15% from other fields.

Fig. 6. Respondents who are unaware about password security.

Argument 3: Computer graduates / computer literate user know the fact that reusing same password decrease password security but still they reuse the same password

We also examine that 31% of the respondent of online survey were Computer Science and IT undergraduates. It was observed from the data collected from online survey that 22% of CS and IT Student were using similar passwords for multiple websites and 18% of CS and IT Student knew that reusing similar password decrease password security but still they practice utilization of same password. We perceived from this evaluation that this hypothesis is also true.

Argument 4: Mostly users use dictionary word, their personal information, phrases and common names as their password

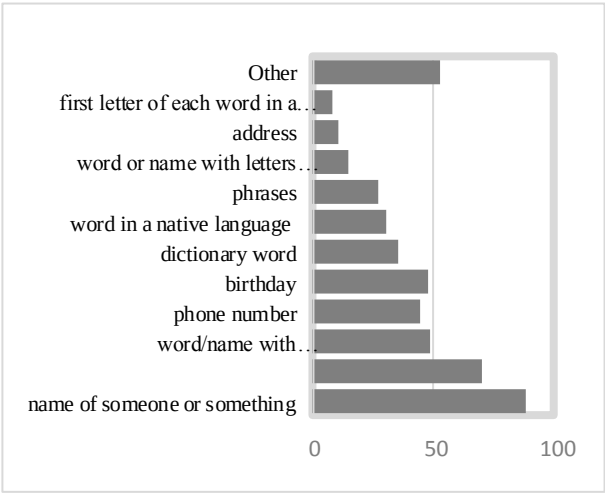

Fig. 7. Percentage of password pattern used by respondent.

We inquired participant in survey that "Which of the following approaches you practice in the process of your password creation?" 35% passwords are constructed using names, 27% word/name with digits, symbol replacing some letters with symbols, 18% create passwords using numbers/symbols added to starting or end to any name/word, 17% passwords used phone numbers , 18% passwords based on birthday ,13% used dictionary word as their passwords,11% created using a word from native language, 10% build their password using phrases, 4% formed using word/name with some letter missing, 3% users used address as their password,2% made using first letter of each word in a phrase and remaining 20% were created using other methods. We observed that 69% of the passwords were created using approach based on names, dictionary word, personal information and phrases by online survey users.

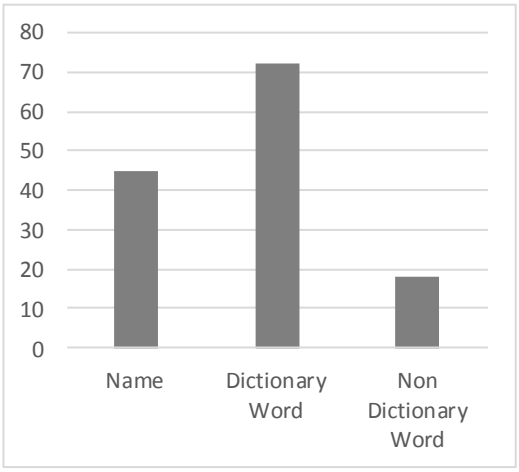

Fig. 8. Categories of passwords patterns.

We further gathered data from experiment one in which 118 accounts were created. Passwords were divided into 3 categories. The first category is name in which we include all the public names, names combined with digits, name with digit and symbol. The second category is based on dictionary words. The third category include non-dictionary word which comprise of symbols with letter and digits, digits and letters and symbols. 34% accounts were created using name category, 53 % accounts were formed using dictionary word category approach and 13% accounts were constructed using non-dictionary word category approach. This proves our hypothesis that majority of users prefer dictionary words, personal information, phrases and common names as their passwords.

Argument 5: Complex passwords created using password policies are difficult to memorize and recall

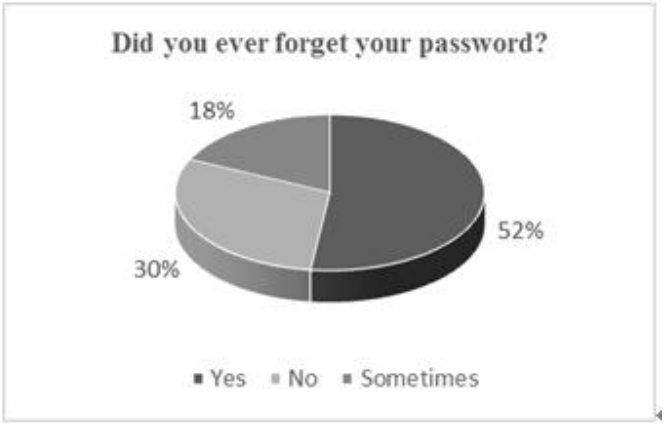

Fig. 9. Percentage of users who forget their password.

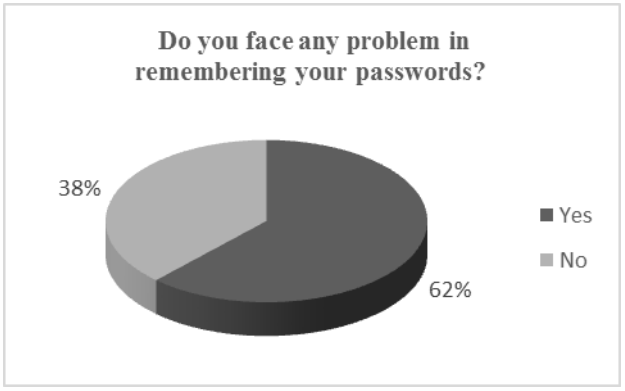

Fig. 10. Respondents answers regarding their password memorability.

Complicated password policies which constrain user to use at least one uppercase letter, lowercase letters, symbols, digits and non-dictionary words are challenging and tough for user to memorize and recall. To prove this hypothesis we asked users "Are passwords with complicated policies difficult to remember?" 62% of survey responder said 'Yes' and 38% said 'No' as shown in Fig. 10.

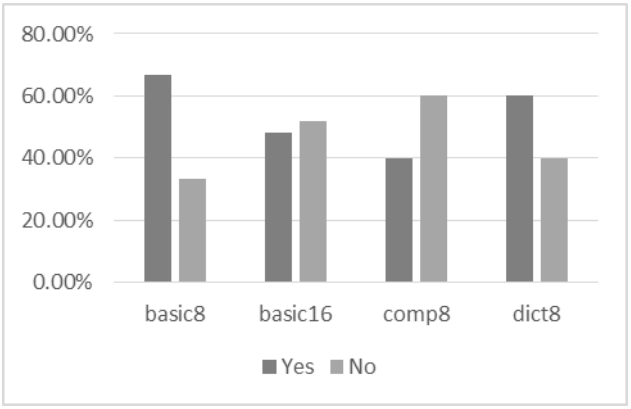

Fig. 11. Will you use this policy in future to make your password secure?

Base8 policy and Dict8 does not constrain the user to use Lowercase letter, Uppercase Letter, symbols, digits, they require at least eight characters, but dict8 constrain to use non dictionary words. These both policies are simple and can easily be memorized as compared to basic16 which requires at least 16 character and Comprehensive8 requires users to use lowercase letter, uppercase letter, symbols and digits. User will prefer to use base8 or base16 for remembrance. This argument attests that password with complex policy are hard to recall thus this hypothesis is proved.

Argument 6: The policies which are more complicated take more time by user to create password

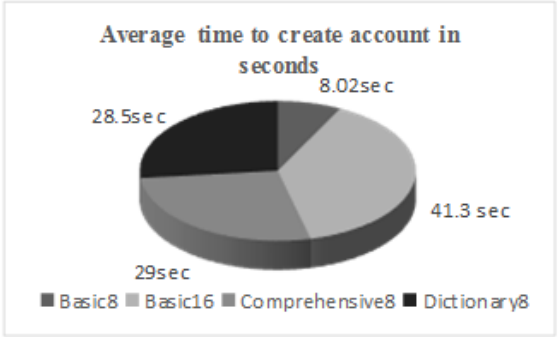

Fig. 12. Average time to create account.

Basic16 policy took more time to create an account because it was too long for users to set the password using basic16 policy. Setting passwords using Comprehensive8 policy was also difficult and users could not create passwords in first attempt.

Argument 7: Different age groups have different type of passwords

We divide our experiment into two age groups of 15-45 and 45 and above. We ask our users to create an account on three different sites namely E-commerce site, E-mail site and a Banking site.

Users from the age group 15-45: Majority of these users created strong passwords for their accounts. They were concerned about the security of accounts and used complex passwords for banking and ecommerce sites.

Users from the age group above 45: Majority of these users created same passwords for all sites.

80% of them said that they use the passwords comprising of name of their children, siblings or wife/husband. They were more concerned about forgetting passwords so they preferred easy to remember passwords that were vulnerable. 70% of the users from this age group used cookies (Website checkbox: "Remember my password on this computer") to remember their password which compromise their password security. Hence, the hypothesis is true that different age group people set different type of passwords.

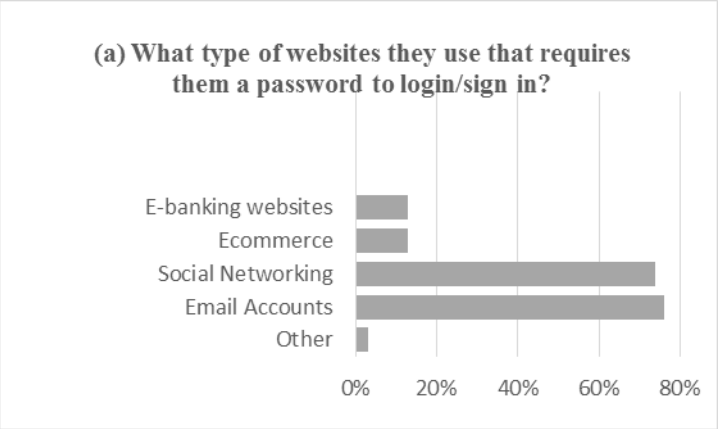

Fig. 13. Types of websites used by responders.

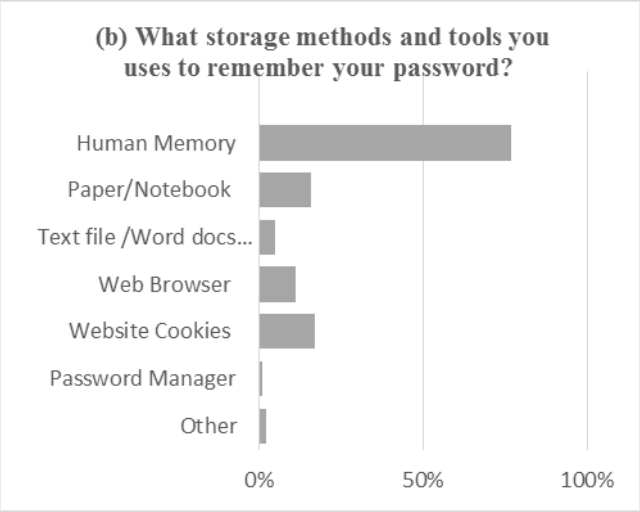

Fig. 14. Password storage methods.

Argument 8: Password meter helps user to create better password

Password Strength meter is an indicator or pointer which can be in graphical figure or it can be in the form of text and it tells the user whether he entered the password which is strong, weak, and medium or the

strongest. Password meter illustrates that how challenging is the password might be to password cracking efforts like dictionary attacks and brute force attack. Password strength meter are made for the motivation of the users to create stronger passwords in the importance of tightened security. To review the strength of password sequence password meter is used. We designed our website with a password meter in it which was based on a comprehensive8 policy. When the users were asked to create an account we provided them a password meter to help them in making strong passwords. Respondents said that although password meter helps them to create a better and strong password but these policy based strong passwords are hard for them to recall. Hence, our hypothesis is true as 85% of respondents agreed that password meters help in creating strong passwords.

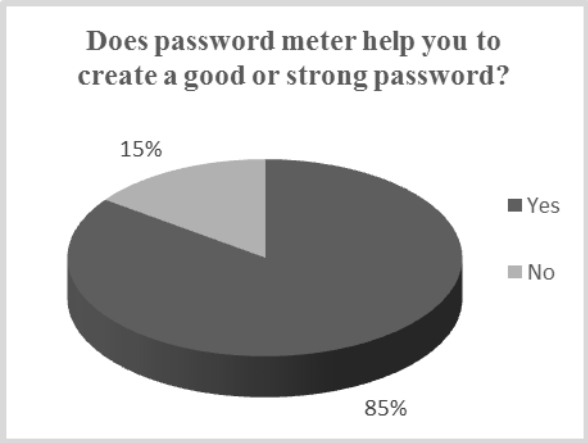

Fig. 15. User response regarding password meter.

6. Conclusion

We investigated the usability of password policies and users' perceptions of password security. We conducted a user study based on experimental evaluation and online survey. During experimental evaluation users were asked to set their passwords using four different password polices that is Basic8, Basic16, Comprehensive8 and Dictionary8. We used multiple experiment set-ups and scenarios to involve users in creating accounts. We concluded that many users prefer same passwords for multiple accounts to reduce the burden of remembering multiple passwords. Such users ignores the threat that their all accounts can be compromised. Also, usability is typically preferred over security and complex password policies annoys user. We also observed that when users are forced to use complex passwords, they tend to reuse same password on multiple sites to improve the memorability of otherwise complex password. Majority of users use family member names, personal information, and dictionary words in their passwords. Such users are not aware of the vulnerability of these passwords. Young users are more concerned about the security of their accounts therefore they prefer to create complex passwords. Password meters are also helpful in making users select strong passwords. However, text based passwords remains a nuisance for typical users and complex password requirements makes it more difficult to remember passwords.

References

[1] Moscaritolo, A. (2016). Hacker selling 32M twitter accounts on dark web. *PC Mag*. Retrieved from http://www.pcmag.com/news/345121/hacker-selling-32m-twitter-accounts-on-dark-web

[2] Johnston, R. (2016). *360 Million MySpace Accounts Leaked Online.* Retrieved from https://www.gizmodo.com.au/2016/05/360-million-myspace-accounts-leaked-online/

[3] Shu, C. (2016). Passwords for 32M twitter accounts may have been hacked and leaked. *TEchCrunch*.

Retrieved from https://techcrunch.com/2016/06/08/twitter-hack/

[4] Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., Cranor, L. F., & Egelman, S. (2011). *Of Passwords and People : Measuring the Effect of Password-Composition Policies.*

[5] Wash, R., Emilee, R., Ruthie, B., & Zac, W. (2016). Understanding password choices: How frequently entered passwords are re-used across websites. *Proceedings of Symposium on Usable Privacy and Security (SOUPS).*

[6] Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). *The Tangled Web of Password Reuse.*

[7] Proctor, R. W. (2002). *Improving Computer Security for Authentication of Users : Influence of Proactive Password Restrictions.*

[8] Shay, R., Kelley, P. G., Leon, P. G., Mazurek, M. L., Christin, N., & Cranor, L. F. *Encountering Stronger Password Requirements : User Attitudes and Behaviors Categories and Subject Descriptors.*

[9] Ur, B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M. L., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N., & Cranor, L. F. *How Does Your Password Measure Up ? The Effect of Strength Meters on Password Creation.*

[10] Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N., & Cranor, L. F. (2016). *Do Users ' Perceptions of Password Security Match Reality ?*

[11] Shay, R., Saranga, K., Adam, D., Phillip, S., Michelle, M., Sean, S., Blase Ur, L., Nicolas, C., & Lorrie, F. C. (2016). Designing password policies for strength and usability. *ACM Transactions on Information and System Security (TISSEC)*, *18(4).*

[12] Kong, H. (2004). *Password Memorability and Security : Empirical Results.*

[13] Cranor, L. F., Hong, J., Reiter, M. K., & Hill, U. N. C. (2016). *Supporting Password-Security Decisions with Data.*

[14] Pinkas, B., & Sander, T. *Securing Passwords against Dictionary Attacks.*

[15] Hanamsagar, A., Simon, W., Christopher, K., & Jelena, M. *How Users Choose and Reuse Passwords.*

Tehreem Hussain has done her bachelor's in computer science from Jinnah University for Women, Karachi Pakistan in 2015. She has been working as a lecturer in computer science and IT Department, Jinnah University for Women for past 5 months. She also worked as a freelance developer and designer. Her research interests include human computer interaction, software engineering and software design and architecture.

Kiran Atta has done bachelors in computer science from Jinnah University for Women, Karachi, Pakistan. She first worked at the Wizards as a QA and business developer for 10 months. Currently, she is working as senior IT officer at Meezan bank in IT department from last 6 months. She also done internship at Meezan bank at Corporate Communication Department as a Meezan website and portal management area.

Narmeen Zakaria Bawany is a Ph.D. scholar in computer science at the National University of Computer and Emerging Sciences, Karachi, Pakistan. She has served as a director of computer science and IT Department, Jinnah University for Women for 12 years. She has over 15 years of teaching experience at graduate and under graduate level. She has supervised many under graduate projects and had also received funding from ICT R&D for under graduate projects. Her research areas include human computer interaction, semantic web, cyber security and software defined networking.

Tehreem Qamar is an M.S. student at NED University of Engineering and Technology, Karachi, Pakistan. Her research interests include machine learning, semantic web and human computer interaction. In 2015, she graduated from Jinnah University for Women with first position and currently working there as a lecturer.