Journal of Computer Science

Original Research Paper

Evaluating Password Behavior at a Small University

[1]Mohammed Awad, [1,3]Zakaria Al-Qudah, [2]Sahar Idwan and [1]Abdul Halim Jallad

[1]*Department of Computer Science and Engineering, American University of Ras Al Khaimah, RAK, UAE*
[2]*Department of Computer Science, Hashemite University, Jordan*
[3]*Computer Engineering Department, Yarmouk University, Irbid, Jordan*

Article history
Received: 30-06-2018
Revised: 03-12-2018
Accepted: 3-01-2019

Corresponding Author:
Mohammed Awad
Department of Computer Science and Engineering,
American University of Ras Al Khaimah, RAK, UAE
Email: mohammed.awad@aurak.ac.ae

Abstract: No matter how sophisticated an organization's security system is, it remains vulnerable due to the human factor. In this study, we surveyed and analyzed the patterns practiced by users when generating passwords at a small-sized university. We found that users are not as aware of security requirements and practices as they think. Moreover, the vast majority of users' passwords are breakable within days or shorter. Interestingly, we found that the use of numbers and uppercase letters is prevalent among users. However, numbers are mostly used at the end of the passwords and uppercase letters are mostly used at the beginning of passwords. The existence of such trends makes it easier for attackers to generate more effective dictionaries. Based on the analysis in this study, we make recommendations to the IT department to improve the password policy. Additionally, we provide recommendations to the faculty, staff, and students on how to strengthen their passwords.

Keywords: Password, Security, Strength, Awareness, Vulnerability

Introduction

Despite many concerns surrounding their security, text passwords remain the most commonly used authentication methods. Since complicated text passwords can be hard to remember, users tend to choose simple passwords. Consequently, these passwords are easier to guess (Gaw and Felten, 2006). On top of that, people tend to reuse the same password across different accounts in order to minimize the number of passwords they must remember (Das *et al*., 2014). While some falsely believe that this might be acceptable if the password is extremely complicated, such behavior may result in additional vulnerabilities since any social engineering, shoulder surfing, phishing attempt, or database breach could jeopardize multiple independent accounts for the same user. This is especially true if the password is stored in plaintext format in one of the databases, which defeats the purpose or the need for a complicated password. Furthermore, users tend to use dictionary words as passwords, which would reduce the effort spent by an attacker to guess them. To counter this, systems usually require users to comply with a complex password policy that may require the user to use non-dictionary passwords with minimum length and a certain combination of uppercase letter, special characters (symbols) and numbers.

Continuous monitoring of user password trends is very important since the development of new patterns may reduce the effort needed by attackers to guess passwords. Therefore, we conduct this study in a university community with the following objectives in mind:

1. Uncover any important trends in user-selected passwords
2. Evaluate the level of awareness that a university community has about the security of their passwords and correlate this level of awareness to the security of their passwords
3. Understand how different factors such as gender, occupation, school and years of affiliation affect the security of passwords
4. Propose appropriate recommendations to the university community under study and to the public to strengthen password selections

The rest of this paper (extended from Awad *et al*., 2016) is organized as follows: Section II sheds light on relevant work; section III describes our research methodology; and section IV presents our results and findings. In section V, we share our recommendations; and section VI concludes the paper.

Related Work

In this section, we briefly review the work that is most relevant to this study. Dell' Amico *et al*. (2010) studied the likelihood of an attacker's guess to succeed in recovering a password using known tools and datasets. They found that the principle of diminishing

Science Publications

returns applies to this case. In other words, attackers are able to quickly guess weak passwords. As the attack goes on, the probability of a guess succeeding diminishes by order of magnitude.

Kirsi and Bakas (2013) conducted a national survey in Norway to assess the level of education that is given to users about the security of electronic devices. Their findings indicate that proper education is not provided, which leads to outdated user behavior. This outdated user behavior may reduce the effort needed to guess passwords from the side of the attacker.

Mazurek *et al.* (2013) conducted a study on a university campus with 25,000 users. The authors had indirect access to the plaintext passwords of these users and, therefore, were able to study how guessable these passwords would be to a state of the art dictionary attack. The authors correlated the strength of user passwords to various factors including demographic and behavioral ones. The authors also concluded that the strength of the passwords of which they obtained access is similar to that of the passwords available for research provided that they were created under similar composition rules.

A national survey in the United States of America revealed that users are generally careless about their choice of passwords despite their growing dependence on electronic means of conducting business (CSID, 2012).

Shen *et al.* (2016) studied password practices of users via an empirical analysis of a large data set of passwords leaked from a software developer network site. They found that passwords are longer than before and a significant increase in the use of combo-meaningful data as passwords, among other findings.

Ur *et al.* (2017) the authors developed and evaluated a password complexity meter that provides detailed feedback to promote the use of more complex passwords. The meter is designed based on a model of password-guessing attack using neural networks combined with 21 heuristics. They found that a detailed feedback meter leads to generating more complex passwords while maintaining the memorability of these passwords.

Our study complements these studies by attempting to reveal the latest trends in user behavior concerning the selection of their passwords. Moreover, we evaluate the correlation between users' self-assessed awareness of security and the actual strength of passwords. Our findings indicate that people believe themselves to be much more knowledgeable of password security than the strength of their passwords actually indicates.

Methodology

To achieve these objectives, we conduct this study at a small university with around 800 students across three different schools (Arts and Sciences, Business and Engineering). In this study, we study the passwords used to access university accounts by over 140 users (faculty, staff and students). These passwords serve as the main and only entry point to all end users. For example, a single password enables a user to log into on-campus computers, university email, the learning management system, the grading system, as well as the HR system when applicable. The university's password composition policy is not very strict. Other than a minimum length of six characters for staff and faculty and eight characters for students, we found no other restrictions. However, the first time they set their passwords, students receive verbal instructions (recommendations) to make them eight or more characters long and to include special characters, numbers and uppercase letters. Additionally, users are permitted a maximum of seven unsuccessful login attempts

We launched a voluntary questionnaire to provide some insight into the password habits of the users. We interviewed 142 participants from all over the campus, of whom only three participants refused to cooperate fully.

The questionnaire was straightforward and gathered general information about the users and their chosen passwords. The questions aimed to find the password length; the use of uppercase letters, special characters and digits; and the position of these less commonly used characters. Furthermore, the questionnaire included questions about the frequency of changing the university password, the use of the same password for other online accounts and whether the subjects suffered from any hacking attempts in the past.

Additionally, the survey participants were asked to insert their passwords into Kaspersky Lab's Secure Password Check (Kaspersky, 2016) to estimate the time it would take a personal computer to crack the inserted password. While we could not find information about how the tool works, we believe that it estimates the time needed to crack (break) the password using brute force and dictionary attacks. In other words, it is assuming the password cracker has a list of commonly used passwords that it compares the inserted password against and if it is not in the dictionary, it will show the time it would take to try out all the possible combinations of that maximum length. For example, "helloworld" would take 3 min to crack since it is in the dictionary, versus 15 days for "helloworl," which is a shorter password, but not a dictionary entry. Notice that in order for us to guess "helloworl," which is a nine character password, knowing that it only consists of lower case letters, would take a maximum of 26^9 guesses, yet if it contained a combination of lower and upper case letters (52); digits (10); and special characters (33), for a password of the same length, the number of all possible guesses would increase substantially to 95^9. Also, the survey subjects were asked to evaluate their knowledge and awareness of Internet security on a scale from one to ten.

Table 1: Statistics of the participants in this study

Category				Total
Gender	Male	Female		
	86	55		141
Class	Student	Faculty	Staff	
	93	33	12	138
Years of	1-2	3-4	> 4	
affiliation	89	36	13	135
School	Engineering	Business	Arts & Sciences	
	69	32	28	129

Table 1 shows basic statistics gathered from the participants, some of whom did not answer all questions resulting in different totals per category.

Results

Our findings are presented in this section:

A. Self-Assessed Awareness

In order to get an idea on how users view their knowledge and of security issues when using Internet services, we asked participants to rate their awareness on a scale from 1-10 with one being entirely unaware of security-related issues and ten being very aware of security issues. Figure 1 shows the results. As shown, the average (self-assessed) awareness score for all participants is 6. Furthermore, staff and participants with over four years of affiliation with the university rate themselves as more aware than other groups. This relatively high self-awareness rating might be related to the fact that 85% of participants believe they have never been compromised. Since most of the participants have never been victims of hacking, they assume that they possess the proper knowledge of password security.

B. Password Characteristics

In our survey, we gathered some input regarding user passwords with a focus on its length, presence and position of special characters, numbers, and uppercase letters.

Figure 2 shows the average length of passwords for all participants as well as a breakdown of the average password length for different groups. As seen, the average password length for all participants is 9.95 characters. Females tend to use slightly longer passwords than males and students tend to use longer passwords than faculty and staff. People with 3 to four years of affiliation with the university use shorter passwords and finally, participants from the School of Arts and Sciences use longer passwords than those from the other two schools. We note here that several factors may affect these results. First, the university encourages the use of complex passwords (even though it's not technically enforcing their use). At the time of registration, users are asked to select at least eight characters long passwords. However, we found that a few faculty and staff passwords were made up of less than eight characters. Second, students seem to be educated about the importance of a long password at the time of setting their passwords. However, similar education is not available to other user groups. It is interesting, however, that the participants from the School of Arts and Sciences use longer passwords than other schools even though computing related programs belong to the School of Engineering.

Next, we examine the presence of special characters (symbols) in the user selected passwords. Figure 3 shows the results. As can be seen, less than a third of all users used a special character. Furthermore, while the percentages are generally similar across all groups, only approximately 15% of participants from the School of Arts and Sciences tend to use special characters. If they used a special character, we asked participants about its position (location) within the password. We found that 75% of the respondents place the special character in the middle of their password (in a position other than the first or last characters).

A similar assessment was performed for the presence of numbers in user passwords. Figure 4 shows the results. Just above 90% of all users use numbers. Similar percentages are found across groups except for people with greater than four years of affiliation where just below 80% of them use numbers in their passwords. Furthermore, close to 65% of total participants place numbers at the end of their passwords.

The results for uppercase letters are somewhere in between. Figure 5 shows these results. Between 30% and 67% of participants use uppercase letters. Furthermore, over 80% of those users place the uppercase letter at the beginning of their passwords.

C. Password Strength

Next, we assess the strength of the user-selected passwords and correlate the results to the awareness level that users reported.

Figure 6 shows the percentage of users whose passwords will take less than one hour, hours, days, months, years and centuries to break for all participants as well as a breakdown of these percentages according to the designation. As can be seen, the majority of passwords (60%) can be cracked within days. Very few passwords would require centuries to break (i.e., effectively non-feasible to break). Around 20% of passwords across designations require years to break. The staff seems to have the weakest passwords. The next chart (Fig. 7) shows a breakdown of password strength according to school affiliation. As seen, the majority of participants in each school have passwords that are breakable within days as well. However, the School of Engineering participants have the largest percentages in the years and centuries categories.

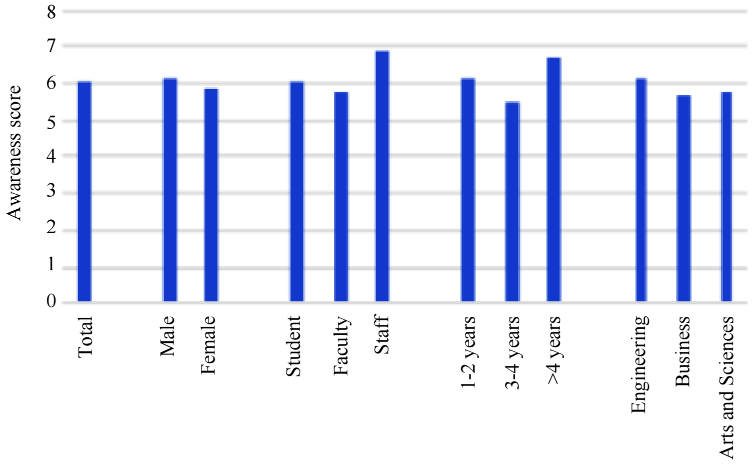

Fig. 1: User's self-rated awareness (1-10), with ten being the highest

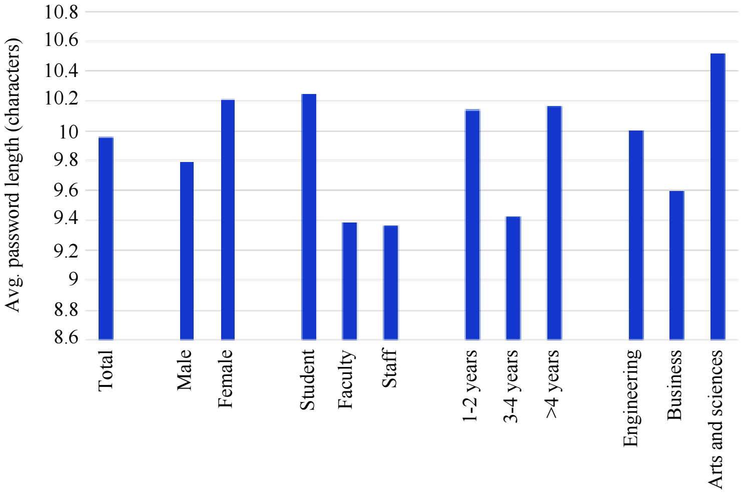

Fig. 2: Average password length for all participants and breakdown along gender, designation, duration of affiliation and school

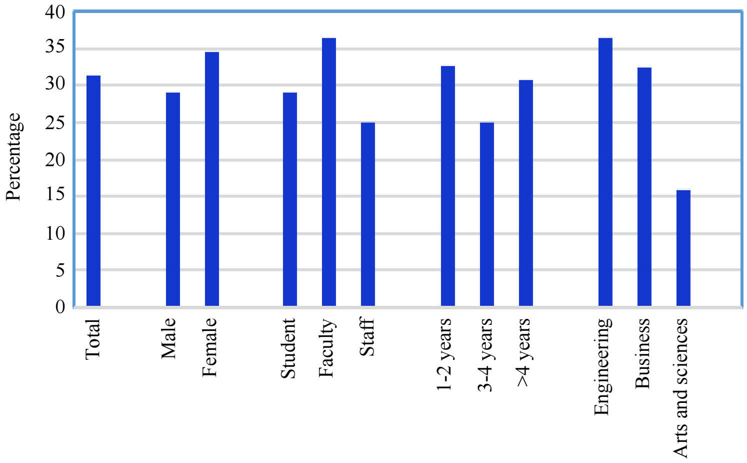

Fig. 3: Percentage of passwords containing special character for all participants and a breakdown along gender, designation, duration of affiliation and school

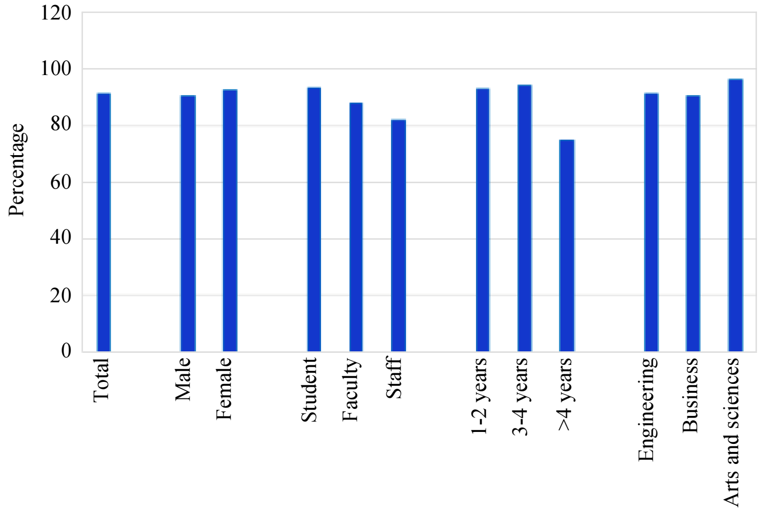

Fig. 4: Percentage of users using numbers in their passwords as well as the breakdown of these percentages across groups

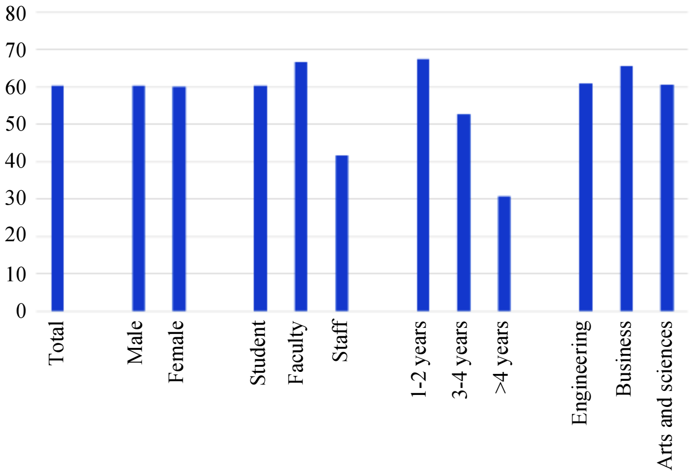

Fig. 5: Percentage of users using uppercase letters in their passwords as well as the breakdown of these percentages across groups

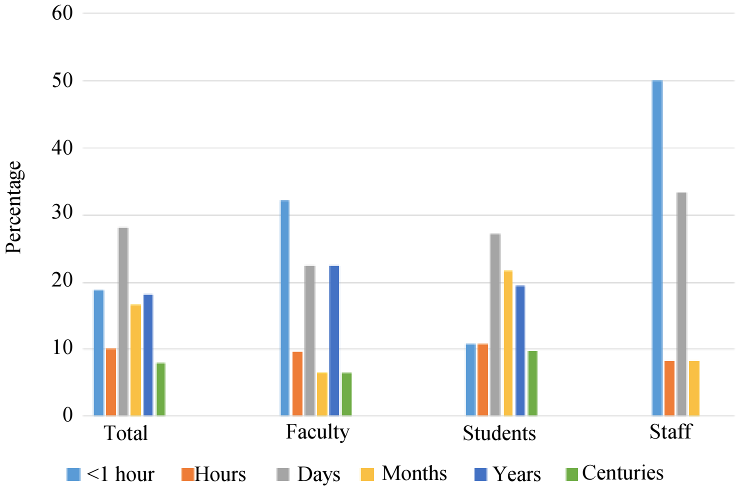

Fig. 6: Password strength for all participants as well as a breakdown of the password strength according to designation

We have also computed the correlation between user self-rated awareness and the strength of passwords. We found a weak correlation (correlation coefficient of 0.13) between the two results indicating that people tend to overrate themselves. This is perhaps due to a misunderstanding of security concepts or due to the fact that most of the participants believe they have never before been victims of hacking.

Additionally, the questionnaire included other data, which provided a better understanding of the participants' actual knowledge and awareness of password security. For instance, we found out that only 58% of the participants changed their passwords at least once and, on average, these participants changed their passwords 2.02 times. Also, the survey showed that nearly 35% of participants who changed their passwords chose similar new passwords.

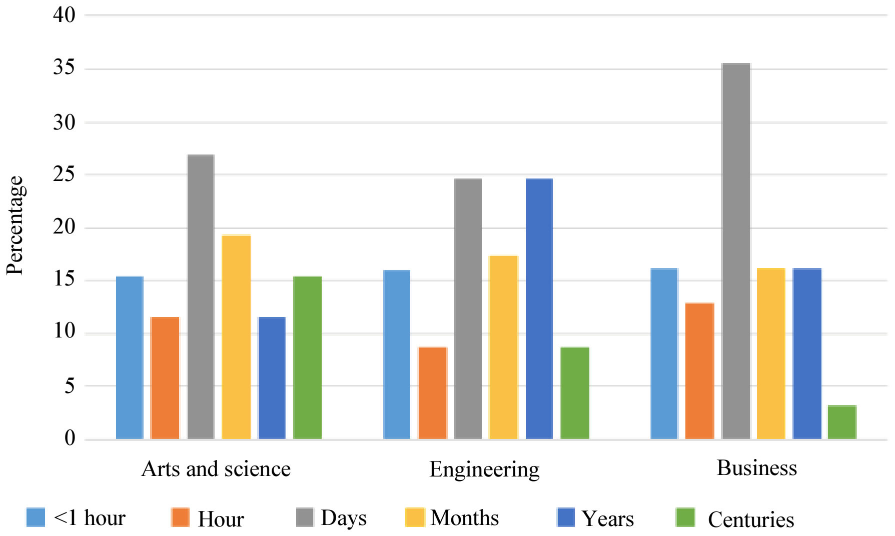

Fig. 7: Breakdown of password strength based on school

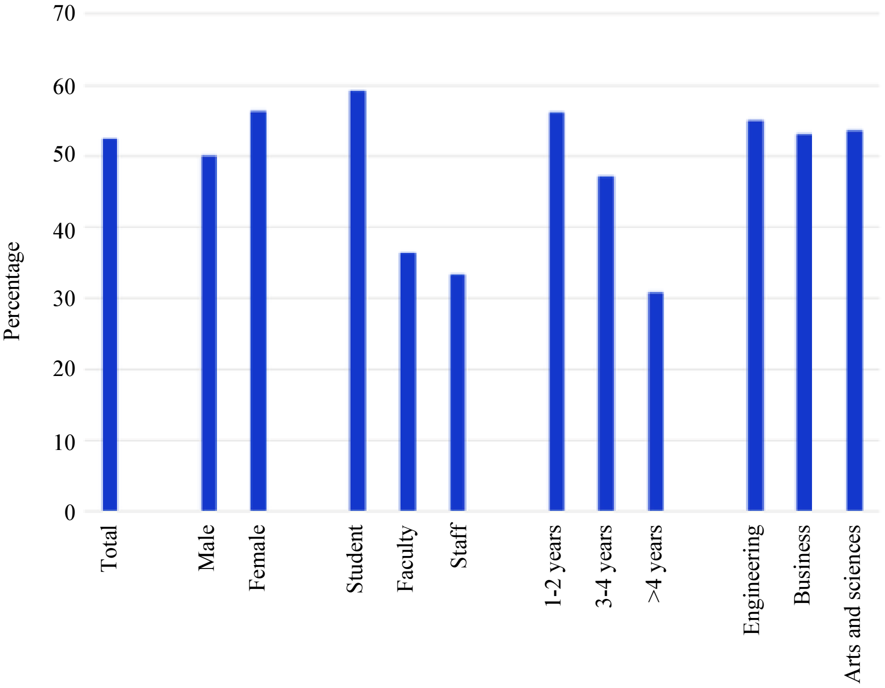

Fig. 8: Percentage of participants reusing the same password for multiple accounts

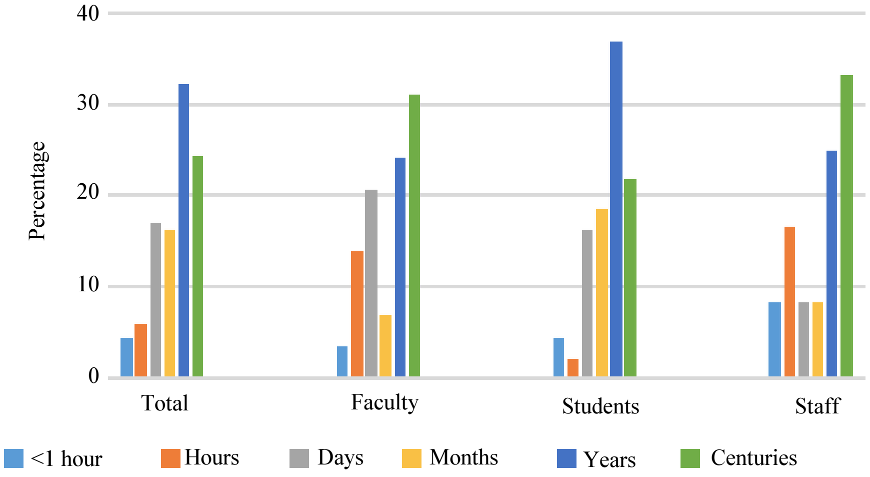

Fig. 9: Password strength after adding '?' at the second position in the password, as well as a breakdown of this strength based on designation

D. Password Reuse

As we mentioned earlier, reusing passwords across multiple accounts can multiply the impact of password cracking. Therefore, we next assess the average number of accounts for which our participants use the same password. Figure 8 shows the results. As seen, just over half of the participants use the same passwords for multiple accounts, which is similar to the results reported by Das *et al*. (2014) Moreover, students tend to reuse their passwords the most frequently whereas people with over four years of affiliation with the university tend to reuse the passwords the least often (about one-third of them reuse passwords). Unfortunately, this habit is widespread since it is estimated that the typical Internet user has 25 online accounts that require passwords (Florencio and Herley, 2007).

E. Strengthening the Password

In order to highlight the importance of special characters in increasing the password complexity, we asked all participants to insert a question mark '?' in the second position and reevaluated the strength of the new passwords. We decided to choose the second position since some dictionary attacks might be able to eliminate special characters in the first and last positions.

Figure 9 shows the result. Adding a question mark at the second position clearly improves password strength significantly. For example, around 55% of passwords now require years or centuries to crack compared to only about 25% without the '?' symbol.

Please note that while adding any character in the second position increases the password strength, a special character might be easier to recall and will result in a password that most likely will not exist in a dictionary.

Recommendations

Based on the results of this study, we propose three recommendations. The first recommendation is to enforce a smarter more complex password policy. For example, the policy should require a minimum length password with a combination of uppercase, lowercase, numbers and symbols. However, uppercase letters should be placed in other locations, not just in the beginning. Numbers should also be placed somewhere in the middle of the passwords. Also, it would be very helpful if the system performed an automatic check and compared the proposed password to common dictionaries before approving it. The second recommendation would be to enforce a periodic password change. Furthermore, the National Institute of Standards and Technology (NIST) listed several electronic authentication guidelines, which increase the password guessing difficulty (Burr *et al*., 2006).

The third recommendation is to properly educate users about computer security and the importance of a strong password. As the results of this paper show, users have a false sense of security. The properties of a strong password were discussed with survey participants, who were then informed how to update their passwords accordingly and on how to compose a memorable yet complex password. However, given the high stakes and widespread security breaches, a proper and continuous education of the importance of selecting complex passwords remains essential.

Conclusion

In this study, we studied the user behavior with respect to password selection in a small university. We assessed the strength of user-selected passwords and computed the correlation between the strength of these passwords and the self-rated awareness of security concepts. In general, we found that around 60% of user passwords could be compromised within days. Note that the compromise duration estimate is a generous one based on an attacker with access to an average personal computer. If the attacker were able to utilize a zombie army, such a password could be compromised within seconds. Furthermore, only around 30% of users use special characters. When present, special characters tend to be placed somewhere in the middle of the password (neither at the beginning of the password nor at the end). Numbers and uppercase letters are much more widely used. However, uppercase letters are typically used at the beginning of the passwords and numbers are typically placed at the end of the password making it easier for attackers to create more effective dictionaries with properties that align with these habits.

Acknowledgment

The authors would like to acknowledge the American University of Ras Al Khaimah for its financial support of the study.

Author's Contributions

Mohammed Awad: Designed the research plan, organized and ran the survey, contributed to the presentation and analysis of the results, added and reviewed genuine content where applicable.

Zakaria Al-Qudah: Designed the research plan and organized the survey, made considerable contributions in interpreting the data and analyzing the results, contributed to the presentation, added and reviewed genuine content where applicable.

Sahar Idwan: Made considerable contributions to this research by critically reviewing the literature review and the manuscript for significant intellectual content.

Abdul Halim Jallad: Supervised the study and made considerable contributions to this research by critically reviewing the manuscript for significant intellectual content.

Ethics

The authors confirm that this study did not result in any privacy violations. Furthermore, participants were educated about the purpose of the survey and its associated risks and were given immediate feedback regarding their password strength and how they might be improved.

Additionally, the authors confirm that the article is an extended version of Awad *et al.*, 2016 as cited. The expanded portion contains new unpublished material; hence, there are no ethical issues associated with its publication.

References

Awad, M., Z. Al-Qudah, S. Idwan and A. Jallad, 2016. Password security: Password behavior analysis at a small university. Proceedings of the 5th International Conference on Electronic Devices, Systems and Applications, Dec. 6-8, IEEE Xplore Press, Ras Al Khaimah, UAE, pp: 1-4. DOI: 10.1109/ICEDSA.2016.7818558

Burr, W.E., D.F. Dodson and W.T. Polk, 2006. Electronic authentication guideline. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-63ver1.0.2.pdf

CSID, 2012. Consumer survey: Password habits a study of password habits among American consumers. CSID.

Das, A., J. Bonneau, M. Caesar, N. Borisov and X. Wang, 2014. The tangled web of password reuse. Proceedings of the Network and Distributed System Security, Feb. 23-26, San Diego, CA, USA, pp: 1-15.

Dell' Amico, M., P. Michiardi and Y. Roudier, 2010. Password strength: An empirical analysis. Proceedings of the Proceedings of the IEEE INFOCOM, Mar. 14-19, IEEE Xplore Press, San Diego, CA, USA, pp: 983-991. DOI: 10.1109/INFCOM.2010.5461951

Florencio, D. and C. Herley, 2007. A large-scale study of web password habits. Proceedings of the 16th International Conference on the World Wide Web, May 08-12, ACM, Banff, Alberta, Canada, pp: 657-666. DOI: 10.1145/1242572.1242661

Gaw, S. and E.W. Felten, 2006. Password management strategies for online accounts. Proceedings of the 2nd Symposium on Usable Privacy and Security, Jul. 12-14, ACM, Pittsburgh, Pennsylvania, USA, pp: 44-55. DOI: 10.1145/1143120.1143127

Kaspersky, 2016. Kaspersky lab's secure password check. kaspersky.com.

Kirsi, H. and T.H. Bakas, 2013. National password security survey: Results. Proceedings of the European Information Security Multi-Conference, May 8-10, University of Plymouth Press, Lisbon, Portugal, pp: 23-33.

Mazurek, M., S. Komanduri, T. Vidas, L. Bauer and N. Christin *et al.*, 2013. Measuring password guessability for an entire university. Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, Nov. 04-08, ACM, Berlin, Germany, pp: 173-186. DOI: 10.1145/2508859.2516726

Shen, C., T. Yu, H. Xu, G. Yang and X. Guan, 2016. User practice in password security: An empirical study of real-life passwords in the wild. Comput. Security, 61: 130-141. DOI: 10.1016/j.cose.2016.05.007

Ur, B., F. Alfieri, M. Aung, L. Bauer and N. Christin *et al*., 2017. Design and evaluation of a data-driven password meter. Proceedings of the CHI Conference on Human Factors in Computing Systems, May 06-11, ACM, Denver, Colorado, USA, pp: 3775-3786. DOI: 10.1145/3025453.3026050