Password Usage: An Analysis in Academic Institution

Mohd Nizam Mohmad Kahar[1], Abdullah Mat Safri[1], Siti Zanariah Satari[1] and Mohd Fadli Zolkipli[1]
[1]Fakulti Sistem Komputer & Kejuruteraan Perisian,
Universiti Malaysia Pahang
Karung Berkunci 12, 25000 Kuantan, Pahang.
mnizam@ump.edu.my, abdullah@ump.edu.my, zanariah@ump.edu.my, fadli@ump.edu.my

Abstract — Password is use widely as an authentication method as access control to resources. Password is preferable because it is convenient and economical compared to other authentication method. Some critical systems, e.g. banking system are geared up to cater the password usage while other solely depends on the user to protect their account. Hence, user could not rely solely on the password system. They also have to take part in assuring a protection towards their resource. Therefore we have surveyed the level of awareness or knowledge of the user on the password usage. This paper discuss on the awareness of the password usage as an authentication method. A survey is carried out among the students, and staff to find out their level of awareness on the password usage. Based on the statistical analysis carried out on the data gathered, revealed that most of the respondent aware of password attackers and know the risk involve if the resource being breach. Besides that, least respondents were taking preventive action in securing their password. As a conclusion, the user need to aware of any preventive action in securing their password. Besides that, it is important to educate the user in ensuring a low risk of violation into the resources. Policies of password usage also should be implemented in assuring an increase in the level of security. We also propose a second line of defence to increase the level of security toward the resources.

INTRODUCTION

Password is a well-known authentication method used nowadays(6,7,9). Password is a security mechanism consisting of a protected or private string of characters known only to the authorized user and the system(2,7,10,12). It is used to authenticate the authorized user of a computer or data file. Password is preferable because it is convenient and economical(6,8). The used of password system required users to choose any combination of characters from a keyboard as their password(4). This password is stored in database for verification purposes(8). Password usually combines with user ID to form a user authentication method(3,8).

Example of password implementation is the used of username and password for login into web-based system. It is a compulsory requirement if there is a need to have an account for authorized access or to authenticate private use only (i.e., universities students' online system). Other examples include wireless AP (access point) where wireless security standard called WPA (Wi-Fi Protected Access) used password to protect the connection from being used by unauthorized or public user(1).

Password is used as a defence mechanism against intruders(5). Password attackers or someone who try to intrude into password protected system will always think of a way to defeat the system. Some of attacks that could be launched to a password such as brute-force attack(8,12), replay attack(5), dictionary attack(7,12), password cracking(11) and social engineering(8,12) (by gathering of password related information). Therefore questions arise, how do we protect our self from password cracker or what action must be taken to cater user with lack of knowledge about good/bad password? Or simple question such as how do we secure our password? Therefore this paper intended to analyze the password usage in academic institution.

MOTIVATION

Nowadays, many systems were developed using password or anything that construct a simple secure login to protect their resources. Hence, users got overwhelmed by the things to remember including their password and lastly dependent on the system to secure their resources.

There are many techniques involved in the password scheme to strengthen the security. Most popular technique is encrypted password(7) and hashed password(5,6,7). Both of the techniques are designed to eliminate an attacker or intruder from easily guest the password used. All these techniques are the mechanisms to strengthen the password in the context of how the password is stored in computer, transferred in data communication line and not in its original state at the time it is stolen. Up to now, the password is strengthening by the technical specification or the algorithm that supports the encoded version of the password itself.

User unaware that the system equipped with password provided, will only help in strengthening the password in term of the structure and mechanism. Hence, neglecting the understanding of what is good and bad usage of password. Therefore, the user would neglect their duty as the resource owner to educate and aware to the policies and procedure on a good password practice. User would simply create password without any evaluation and in the end leads to picking up a simple guessable password. This way would make less painful for the password cracker compare using a well construct password. Therefore this paper constructed, to study and analyze the level of knowledge about password usage and the practical used of the password in academic institution.

METHODOLOGY

The questionnaires are distributed among the students and staffs in Universiti Malaysia Pahang (UMP) to gather their views. This survey is open to all students in all level of studies and faculties. Staffs are defined as academic and support staff. By doing so, we hope to gather as much data and opinion on the password usage as an authentication method. The questionnaires are distributed to the students through their lecturers. While for staffs, the questionnaires are distributed through their faculty office. After determining the targeted respondents, only than the questionnaires are distribute.

The questionnaire is categories into two main aspects; the first aspect is the (a) knowledge in password. Here, the questions concern on the level of knowledge of the respondent on the password. Questions being address such as, the best practice of password, the suitable number of password, usage of number or character alone or a combination of number and character (or special character) in password, usage of private information as password, do they aware of the password attackers and source of information update. Second aspect is the (b) Practical usage of password. In this area, the questions concern the usage of password with respect to knowledge. Questions being address such as used of default password (given by admin), applied the knowledge in section (a) in the use of password, write down password or tell someone else, using same password for electronic transaction (that uses password) and frequency changes of password. From the questionnaire, we hope to capture the level of knowledge, usage, user behaviour and comment in the use of password as an authentication method. Through this, a better ways in upgrading the security of password could be achieved.

RESULTS AND DISCUSSION

The result is discussed with respect to the relation between categories of respondent and their knowledge on bad password, password cracker and practical aspect. All the data gathered from the questionnaires has been analyzed by using SPSS 10.0 for Windows statistical software package. Analysis is carried out using several statistical methods such as Cross-Table and Correlation.

Fig. 1 shows the pie chart for the number of respondents. Around 62.5% students and 32.5% staffs responded to the survey.

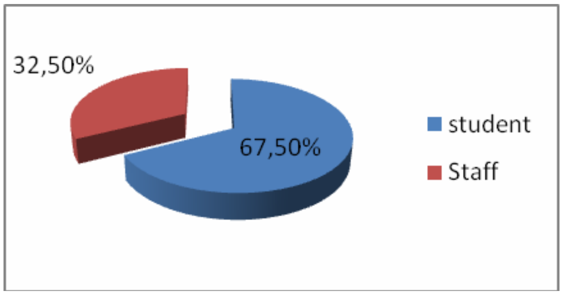

Fig. 1. Percentage of respondent.

Knowledge on Bad Password

In this section, we are going to look at the relation between categories of respondent and their knowledge about bad password. Referring to Table 1, between 30.8% to 50% or less than half of UMP's student have minimum basic knowledge about bad password. Minimum basic knowledge means know at least one of six knowledge about bad password.

For UMP's staff, about 32% to 84% of the respondents have minimum basic knowledge about bad password. This showed that staff's knowledge about bad password is higher compare to student's knowledge. However, 68% of staff did not know the usage of foreign language as password is bad compared to student with 65.4%. It is also found that most of the student and staff know about the combination of alphabet, number and character to produce password is good compared to other knowledge.

Table 1 Percentage of Respondent Agree

Question	Student	Staff
a. Know about bad password	17.3%	44%
b. The usage of 8 or more digits in password is good	46.2%	68%
c. The combination of alphabet, number and character to produce password is good	50%	84%
d. The usage of foreign language as password is bad	34.6%	32%
e. The usage of number only as password is bad	30.8%	64%
f. The usage of alphabet only as password is bad	32.7%	64%
g. The usage of personal information as password is bad	48.1%	72%

Password Cracker

Here, we are going to look at the relationship between respondent categories and level of knowledge about password cracker. Based on the surveyed, staff's knowledge on the existent of password crackers is high compared to student. The percentage of staff knowing the method to crack password is also high compared to student, however the percentage difference is not that large. Refer to Table 2.

Table 2 Summary Surveyed on Password Cracker

Question	Student	Staff
Aware on the existent of password crackers.	63.5%	88%
Knowing the method to crack password	13.5%	28%

Meanwhile, through Mann-Whitney analysis we found out that there is no difference in the level of knowledge in password cracking between respondent categories. Therefore we could say that the category of respondent does not affect the level of knowledge in password cracking.

Practical Used of Password with Respect to Knowledge of Bad Password

Here, we examine whether is there a relation between knowledge about bad password with the respondent practical usage of password. Because of the data are in the ordinal form, correlation analysis that is suitable to be used is Spearman's rho Correlation[13].

Table 3 Correlation between Knowledge on Bad Password with the Respondent Practical Usage of Password

Question		Applied knowledge number A2 - A7 in the usage of password
a) 8 or more digits in password is good	Correlation Coefficient	**.323**
	Sig.(2-tailed)	**.004**
b) combination of alphabet, number and character to produce password is good	Correlation Coefficient	**.408**
	Sig.(2-tailed)	**.000**
c) usage of foreign language as password is bad	Correlation Coefficient	-.199
	Sig.(2-tailed)	.083
d) usage of number only as password is bad	Correlation Coefficient	**.262**
	Sig.(2-tailed)	**.022**
e) usage of alphabet only as password is bad	Correlation Coefficient	**.278**
	Sig. (2-tailed)	**.015**
f) usage of personal information as password is bad	Correlation Coefficient	.115
	Sig. (2-tailed)	.320

Bold value: Correlation is significant at the .05 level

Table 3 showed that only small number of respondents applied the knowledge of 8 or more digits in password, combination of alphabet, number and character, and usage of number only and alphabet only as password is bad in the usage of password.

However, correlation value showed that the knowledge about usage of foreign language and personal information as password are bad are not related to the pratical usage of password by the respondent. It means that respondent did not applied the knowledge about usage of foreign language as password and usage of personal information as password are bad in the usage of password.

An interesting finding from the survey is that, some of the knowledge have strong correlation with one another. It showed that:

- Respondent with knowledge about 8 or more digits in password is good also know about combination of alphabet, number and character to produce password is good and usage of number only as password is bad.
- Repondent with the knowledge about usage of alphabet only as password is bad also know about usage of number only as password is bad.

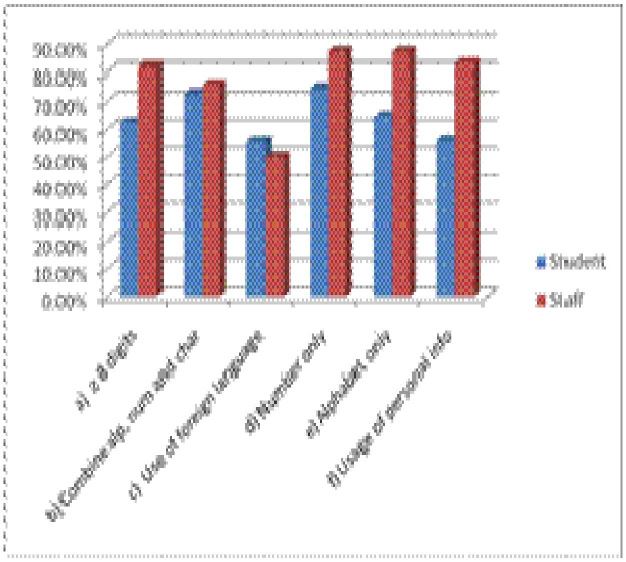

Fig. 2. Percentage of applied knowledge about good/bad password between category of respondent.

Furthermore, from Fig. 2, we notice that between 55.56% to 75% of student really applied the knowledge that they had. While for staff between 50% to 87.5% applied the knowledge they had. Generally, majority of staff applied their knowledge on proper password usage. Most of student and staff applied their knowledge in term of the usage of number only and combination of alphabet, number and character. The lowest practical percentage is at the usage of foreign language as password is bad around 50%.

Overall, staff applied their knowledge about good/bad password in password usage in almost all the items such as the usage of 8 or more digits in password is good, the usage of number only as password is bad, the usage of alphabet only as password is bad and the usage of personal information as password is bad with percentage more than 80%. For student, they applied the knowledge in password usage moderately.

From Fig. 3, small percentage from both respondents who use default password given by system administrator showed that they like to use their own password rather just accept and use the default one which is good. It also showed that they know and aware about the important to change the default password and they applied the knowledge.

Small percentage in the usage of reverse word as password from student and almost none from staff used it in the password usage. It showed that the usage of reverse word as password did not be a preference in password usage and respondents aware about this matter which is good to eliminate easy guessable password.

For next item, small percentage is also found from both respondents that write down password on a piece of paper but, the percentage for student is lower than staff. Although the percentage is small around 6% to 9%, writing down password on a paper is a critical issue in password and supposedly the percentage must be zero. Therefore, any small number of respondents who write their password on a paper maybe results in a big disaster compare to the low percentage.

In the usage of same password for all electronic transaction, student showed high percentage about 75%. This comparison is very considerable where staff only around 18%. This showed that almost all staff used different password for several electronic transaction and student preferred to use the same password. It could be concluded that staff is better in applying their knowledge about good/bad password in creating more than one password compare to student that used the same password for all, although they have the knowledge about good/bad password.

Next item is about giving own password to others. Generally, the percentage is low for both respondents but percentage for student is higher than staff. Although both respondents have knowledge about good/bad password, respondents tend to give their password to others. This showed that there is also misconception in their awareness about usage of password. Maybe, they give it to people them trust but this is not the case in security. Everybody is potential to be victimized even with their close relative.

Overall, all items showed lower percentage and it means almost all respondents applied their knowledge about good/bad password to at least, protect their own password from people easily know their password. Although there is one percentage around 75% from student about using the same password for every electronic transaction, it is not the case if the student could keep the only password securely with proper guidelines.

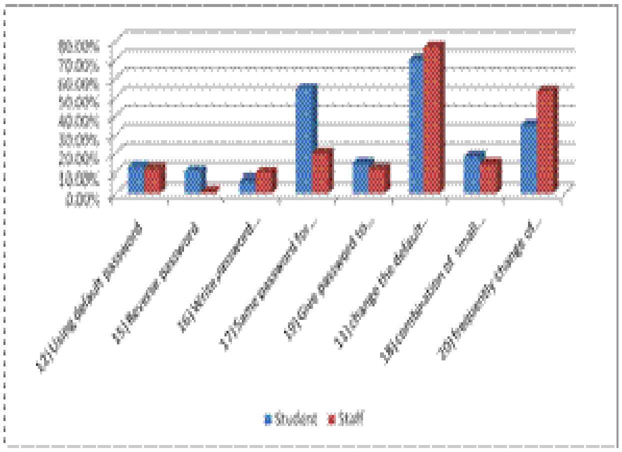

Fig. 3. Percentage of password usage between category of respondent.

From the survey, it also showed that, high percentage of student and staff will change their default password given by system administrator and it means that the respondent applied their knowledge about good/bad password. However, from the analysis before, there exist a weak correlation between knowledge about good/bad password and respondent usage of password. It means, the respondent aware of the importance to change default password but at the same time they did not used their knowledge to do so.

From the analysis, this paper found out that the awareness of usage of password among student and staff are not proper guided. This paper used two questions as an evidence where the percentage for both student and staff that combine small and capital letter in password and frequent change of password are in small percentage. Only half of respondent from staff used their knowledge to change password frequently but at the same time, less respondent used recommendation on good/bad password in the usage of password.

Attempt to Crack a Password

Here, we examine whether there exist relationship between knowledge about the awareness of existance of password crackers and knowledge about password cracking method with the respondent attempt to crack other people password. From the analysis, both, the data for the the awareness of existance of password crackers with the respondent attempt to crack other people password showed that there exist relationship but the number is too small; *r*=0.151. The relationship between password cracking method with the respondent attempt to crack other people password showed that *r*=0.414; there exist relationship between them.

In other words, the awareness among student and staff about the existance of password crackers is low but the second analysis showed that the attempt to crack other people password have better significant. From this analysis, whether the student or staff aware of password crackers are (1) not reliable because of the significant relation on attempt to crack other people password or it is (2) reliable as the student or staff know how to crack other people password but did not aware of what they actually did is so called password cracker. But the percentage of all respondent attempt to crack other people password is less than 35%.

PROPOSE SOLUTION

Based on the result gained, we propose the following action in order to increase the security of password authentication mechanism:

a) User itself has to be responsible on their password and applied proper password usage in order to increase security of password. Therefore, they have to educate themselves with sufficient knowledge and good practice of password by reading related material, attending course, seminar and etc.

b) The system itself need to be ready and equipped with the password policy that enforce the individual to practice good password usage. This is to ensure that the bad password usage among individual whose lack of knowledge (about good password usage) or did not implement the knowledge even they knew it could be avoided.

c) Typing biometric method could be implemented as a second line of defence to further enhance the security of password. This method has been discussed by several researchers and in our preliminary study, we found out that this technique is suitable in eliminating the problem comprehend in (a) and (b)

CONCLUSION

Password is a well known authentication method and widely used because of the convenient and economical features as compare to others security system. People tend to take things (password) for granted where they did not apply proper password usage (prior to their knowledge). Therefore the user, system policy and second line of defence (typing biometric method) must be applied to better enhance overall password authentication system.

REFERENCES

[1] Luo, H. (2000). A Server-Independent Password Authentication Method for Access-Controlled Web Pages. (361-364). IEEE.

[2] Duffy, N. and Jagota, A. (2002). Connectionist Password Quality Tester. IEEE Transactions on Knowledge and Data Engineering, Vol. 14, No. 4, pp. 920-922, July/August 2002.

[3] Harris, J. A. (2002). OPA: A One-time Password System. Proceedings of the International Conference on Parallel Processing Workshops, IEEE.

[4] Mendori, T., Kubouchi, M., Okada, M. and Shimizu, A. (2002). Password Input Interface Suitable for Primary School Children. Proceedings of the International Conference on Computers in Education, IEEE.

[5] Soh, B. and Joy, A. (2003). A Novel Web Security Evaluation Model for a One-Time-Password System. Proceedings of the IEEE/WIC International Conference on Web Intelligence, IEEE.

[6] Esch, J. (2003). Comparing Passwords, Tokens, and Biometrics for User Authentication. Proceedings of the IEEE, Vol. 91, No. 12, pp. 2019-2020, December 2003.

[7] Wang, X., Heydari, M.H. and Lin, H. (2003). An Intrusion-Tolerant Password Authentication System. Proceedings of the 19th Annual Computer Security Applications Conference, IEEE.

[8] Conklin, A., Dietrich, G. and Walz, D. (2004). Password-Based Authentication: A System Perspective. Proceedings of the 37th Hawaii International Conference on System Sciences, IEEE.

[9] Chang, C. C. and Chang, Y. F. (2004). Yet Another Attack on a QR-based Password Authentication System. Proceedings of the 18th International Conference on Advanced Information Networking and Application, IEEE.

[10] Dailey, M. and Namprempre, C. (2004). A Text-Graphics Character CAPTCHA for Password Authentication. IEEE.

[11] Goyal, V., Abraham, A., Sanyal, S. and Han, S. Y. (2005). The N/R One Time Password System. Proceedings of the International Conference on Information Technology: Coding and Computing, IEEE.

[12] Whitman, M. E. and Mattord, H. J. (2004). Management of Information Security. Boston, Massachusetts: Course Technology.

[13] Hishamuddin M. S. (2005). Panduan Mudah Analisis Data Menggunakan SPSS Windows. Penerbit UTM, Universiti Teknologi Malaysia: Johor.