AN ASSESSMENT ON THE PASSWORD PRACTICES AMONG STUDENTS

[1]MOHD ZALISHAM JALI, [2]SHAHARUDIN ISMAIL, [3]ZUL HILMI ABDULLAH

[1, 2, 3]Faculty of Science & Technology, Universiti Sains Islam Malaysia (USIM), Bandar Baru Nilai, 71800, Negeri Sembilan, Malaysia.

E-mail: [1]zalisham@usim.edu.my , [2]shaharudin@usim.edu.my , [3]zulhilmi.a@usim.edu.my

ABSTRACT

User authentication can be defined as the process of proving the user's identity. Three typical categories of user authentication are based on users' knowledge (i.e. PIN and Passwords), users' possession (i.e. Smart Card and Token) and users' characteristics (i.e. Iris and typing pattern). This paper presents an extensive review related to password-based authentication and then reports the latest experimental study conducted to evaluate the password practices among students within the authors' institution. Participants within the study were given a scenario where their accounts were hacked and straightforwardly, they were asked to create new passwords according to three conditions; namely C1 (i.e. having at least one upper, lower, number and special character), C2 (i.e. contains at least three words) and C3 (i.e. combination of C1 and C2 respectively). After a week time, they were again invited to participate by writing down their passwords to investigate memorability. Overall, the study managed to recruit 380 students, having a total of 1140 passwords. From the analysis covering password memorability, password creation and password perception, it could be reported that the three tested conditions have both positive and negative outcomes, thus authors suggest that 'a second look' should be considered if these conditions to be implemented in real setting.

Keywords: *User authentication, Memorability, Password, Knowledge-based Authentication, Vulnerabilities*

1. INTRODUCTION

The function of verifying a user's identity is important in establishing trust in critical business processes. This process, known as authentication is the act of confirming the truth of an attribute of a datum or entity, or in other words, is the act of verifying a person's claim on his or her identity [1] and [2]. In fact, the basis of authentication lies in the principle that without a proper form of identification, a system will not be able to correlate an authentication factor with a specific subject. Liao et al., [3] explain three types of identity authentication methods, including:

a) Accepting proof of identity given by a credible person who has evidence on the said identity, such as password.
b) Comparing the attributes of the object itself to what is known about objects of that origin.
c) Relies on documentation or other external affirmations, such as smart cards and fingerprint.

It is anticipated that proper authentication methods are vital for safeguarding and maintaining the confidentiality, integrity, and availability of the organization's IT infrastructure. The simplest form of authentication is using a combination of username and password. Besides password, there are multiple ways by which users can provide their identity, such as swiping a smart card, waving a token device, or using voice recognition. These authentication tools are categorized as hardware tokens, software tokens, digital certificates on smart cards and USB tokens, challenge response, biometric authentication, and out-of-band authentication [2].

O' Gorman [4] explained user authentication methods into the knowledge-based (something users know), the possession-based (something users have) and the biometric-based (something users are). For the knowledge-based approach, users have something that they must remember; this is usually a pin or password. For the possession-based methods, users have some form of device (e.g. smart cards or 'USB' devices) and for the biometric-based methods; users commonly have to use a physiological characteristic (e.g. their face, finger, thumb, and iris) in order to be authenticated (see Figure 1). This paper concentrates on the password (i.e. text-based password) authentication that is grouped within the knowledge-based method.

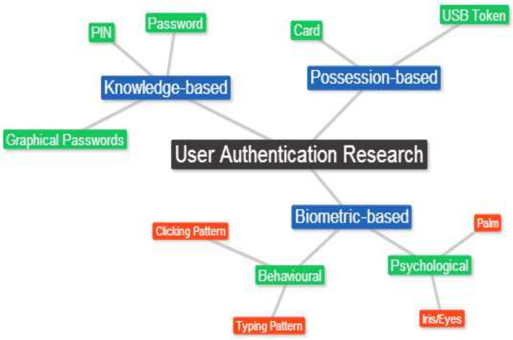

Figure 1: User Authentication Research

This paper is arranged as follows. Section two highlights previous works which authors thought having similarity with the paper, with section three presents the methodology used for data collection. Section four then details out results from the data collection and finally conclusion and references are given for those want to investigate further into the password research.

2. RELATED WORKS

Password research has long been researched and reported, covering various scopes and perspectives. Among earliest attempts were the work reported in [5], [6] and [7]. Identifying human and organisational factor that contributed to the security and usability of password-based authentication system were studied in [8], with Cartens et al., [9] in their work conducted a survey and evaluated the human impact of password practices. Schneier [10] analysed MySpace users' passwords and found nearly 65% of the users' passwords were eight characters long or less. He also reported that some users had passwords that were more than nine characters long, but these passwords were easy to predict. 81% of users' passwords were combination of letters and numbers, with only 1.3% and 9.6% of users' passwords formed using number only and letters only respectively. Although not worrying, users still formed simple and easy to guess password as the author revealed the top twenty common passwords included 'password1' and 'abc123'. Florencio and Herley [11] investigated users' password habits on the web; with the study of collecting larger passwords on webs is found in [12]. Having multiple passwords was also studied and reported, and the most common cited work is in [13].

Yan et al., [14] reported an outstanding study related to users memorability to remember their passwords. Their study provides strong motivation for authors to conduct similar study, but with different settings. Shay et al., [15] focus on users' behavior and attitude in designing better policy for password practice, with Ur et al., [16] used password-strength meters to identify users' behavior during password creation and found the password-strength meters gave positive effect to participants as they create longer and secure passwords. Educating and enforcing users to use more secure password are also part of responsibility of the application service provider. They should guide users by enforcing the password minimum characters, listing the weak password, guiding users with strength password choices as well as embedding graphical password with text based password. The aforementioned study is investigated in [17].

The combination of username and password could easily be broken and vulnerable to several types of attacks such as brute force attacks, dictionary attack, key loggers, phishing attacks, shoulder surfing, replay attack as well as password recording attack [18]. According to Jones [19], there exist three ways an intruder could get other user's password - gain access to the information stored inside the system, intercepting the user's communication with the system, and the user's inadvertent disclosure of his password - and then logging in and interacting with the system. As rapidly growth of hardware and processer technology and speed with advance features of software, password can be cracked easily and make the system authentication vulnerable. In order to mitigate those attacks related to text based password, researcher must identify the method of attack that can be used to exploit vulnerabilities and weaknesses of potential system that used the text password [6].

There are ways to protect the username and password. Enhancing password with cryptographic approach is one of the preferred methods in authentication based research works [20], [21], [22] and [23]. Nevertheless, cryptographic based password is still vulnerable. Researchers then proposed more secure and complex techniques to enhance the authentication process such as using graphical passwords, biometric based authentications, keystroke dynamic, click pattern, virtual password and time signature [18]. In addition, the use remote password authentication scheme using smart cards [24], [25] and [26] and embedding password scheme in hardware or devices (i.e. Trusted Platform Module) in [27] are also being used for more secure authentication process.

Taken these literatures into account, authors suggest that the password problem could be caused by three entities; namely the user, organization (e.g. Internet Service Provider) and even developer itself. The user reuses their passwords, share with others, writing down and create easy to guess passwords. The organisation could contribute to the password problem if they create 'hard to follow' standard and policy such as frequency of password changing and the passwords composition themselves and finally, the developer could also contribute to the password problem if they practice poor design (e.g. poor user interface and poor data storage) during development of the authentication applications (see Figure 2).

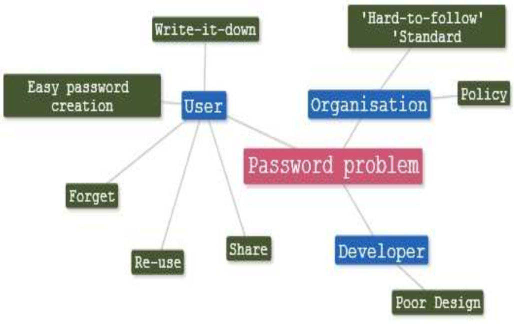

Figure 2: Password Problem

This paper reports an empirical password study conducted to students from the authors institution, with the ultimate aims to obtain students' level of password awareness (did they aware with the need to create strong password?), students' perceptions (how they perceived passwords policies during password creation?) and password creation (how students created/composed their passwords? Is there any pattern when creating passwords according to the defined policies?). To the best of authors' knowledge, the present paper is considered among the latest empirical research conducted. In addition, authors thought that the password research is still worth doing despite user authentication technologies have moved to other means and features (e.g. two-factor authentication and biometric-based) due to the fact that current hardware still equipped with alphanumeric keypads, less cost to deploy, took less time to authenticate and considerable ease of use. In addition, as participants were those from Sciences and Islamic background, with both categories needed to create password according to three specified conditions, authors anticipate that it is interesting to be discussed and reported.

3. METHODOLOGY

The present study used an empirical evaluation type. Specifically, participants were invited to participate where they were given a scenario of their accounts (i.e. email and social networks) were hacked and straightforwardly, they were asked to create new passwords according to three conditions, as explained below.

a) Condition one (having at least one upper, lower, number and special character), C1.
b) Condition two (contains at least three words, e.g. just for fun), C2.
c) Condition three (combining rules from condition one and two respectively), C3.

For all three conditions, they were advised to create their passwords with a minimum of eight characters including the blank space (i.e. this is one of many best practices suggested by well-known organisation such as NIST, Google and Yahoo), and the created password should not be available in any well-known English and Malay dictionaries. This is due to the fact that participants recognise (i.e. speaking and writing) both languages. After a week time, they were again invited to participate by writing down their passwords (i.e. they were told of this during their first trial). The idea of inviting them to rewrite their passwords was to investigate memorability (i.e. ability to recall their passwords).

The reason these three conditions were chosen as for the C1, it is a best practice and normally advised/suggested by organisations to be used for creating secure password, such as the NIST. As for the C2, it is interesting to be researched as Baekdal [28] claimed that this kind of method is not only memorable but 'hard' to crack and with the C3, combining rules from C1 and C2 are thought to making password more secure, with high memorability. The evaluation was conducted on a paper-based, during lecture in the lecture hall of the authors' institution. Steps each participant needed to follow are:

a) Read the information sheet and upon agreement, sign-in the consent form.
b) Start the trial by creating their passwords based upon three conditions, CI, C2 & C3.
c) Answer feedback questionnaire.
d) After one (1) week, invited to re-write their three passwords.
e) Answer feedback questionnaire.

There were two sets of feedback questionnaire distributed to participants. In the first trial, participant were asked to rate the level of difficulty (i.e. ranging from easy to difficult) for each condition, rated the most preferable condition to be used and reason for choosing it. In the second trial, similar questions were presented but this time, participants were asked to rate perceived memorability of their passwords (i.e. ranging from easy to difficult), preference mean for authentication and reason for choosing it. The five-Likert scale was used to obtain their answers and these will be reported in the next section.

In term of the way this research was conducted, it is anticipated that the absorbed method would also produce the same results regardless of the methodology. However, as the trial was conducted in the lecture hall, it is somehow could affect the process and progress of the trial due to students' attendance (e.g. absent during the first trial but not on the second trial and otherwise) and their behaviour (e.g. not serious) while participating.

4. RESULTS AND DISCUSSIONS

Overall, the trial managed to recruit a total of 380 students, with the average age of 20 years old. Specifically, 187 (49.2%) were third year Islamic background students whereas 193 (50.8%) were second year applied science students, respectively. Although total number of female participants (i.e. 276, 72.6%) were larger than male participants (i.e. 104, 27.4%) and resulted in gender based skewed, however it is anticipated that their contribution is still valid for justifying the results.

A total of 1140 plaintext passwords (each participant created three passwords according to three conditions) were collected. The study found that nearly 50 participants (13%) were absent and, thus miss out to participate in the second trial. This section reports findings into three major parts; namely password memorability (i.e. level of recall within two trials), password creation (i.e. common mistakes and common pattern identified during passwords creation) and finally password perception (i.e. participants opinion on the feedback questionnaire). Password strength was not presented as it is anticipated that the three tested conditions should provide effective level of security.

4.1 Password Memorability

Table 1 summarises number of participants correctly writing down (i.e. recall) their passwords in second trials, reported according to conditions. From Table 1, it could be deduced that nearly 32% of participants managed to correctly writing back their passwords for all conditions, with only 11% participants incorrectly writing back their passwords. Of all the conditions, C2 recorded highest memorability rate as 76% participants correctly writing their passwords, with 67% participants and 46% participants correctly writing their passwords for both C1 and C3 respectively. This result was expected due to the fact that C2 only requires participants to create a password based upon word combination, whereas in C3 & C1, participants needed to mix words and numbers and then compose at least three words; which directly have effect on their memory tasks.

Table 1: Participants' Memorability towards Two Trials

Condition, C	Explanation on condition	Number of Participant	Percentage (%)
C1	Only C1 remember correctly	19	5.0
C2	Only C2 remember correctly	42	11.1
C3	Only C3 remember correctly	10	2.6
C1 & C2	C1 & C2 Correct, C3 Wrong	74	19.5
C2 & C3	C2 & C3 Correct, C1 Wrong	15	3.9
C1 & C3	C1 & C3 Correct, C2 Wrong	8	2.1
C1, C2 & C3	Remember C1, C2 & C3 correctly	121	31.8
XX	Absent for the second trial	49	12.9
X	Failed/Uncorrected Attempt	42	11.1
	Total	**380**	**100**

Table 2 extends Table 1 by reporting participants' performance according to their study background; namely Science students, S and Islamic students, I. Overall finding from the Table 2 reveals that participants who study Islamic course performed better as compared to participants who study Science course. Authors anticipate that Islamic students who good at remembering C1 and C3 are expected, since their course requires them to have good memory to memorise contents from Quran and Hadith (i.e. the Prophets words).

Table 2: Participants' Memorability According to their Background.

Condition, C	Participant Background	Number of Participant
C1	Science Participant, S	7
	Islamic Participant, I	12
C2	Science Participant, S	27
	Islamic Participant, I	15
C3	Science Participant, S	4
	Islamic Participant, I	6
C1 & C2	Science Participant, S	36
	Islamic Participant, I	38
C2 & C3	Science Participant, S	6
	Islamic Participant, I	9
C1 & C3	Science Participant, S	3
	Islamic Participant, I	5
C1, C2 & C3	Science Participant, S	59
	Islamic Participant, I	62
XX	Science Participant, S	15
	Islamic Participant, I	34
X	Science Participant, S	24
	Islamic Participant, I	18
	Total	**380**

4.2 Password Creation

This section reports password created by participants, common mistakes identified while composing their password according to three specified conditions, as well as detail out identified patterns while creating passwords. For all passwords collected, only two participants who identified of using the word of 'password' as their password (i.e. although participants were told not to so).

Table 3: Password Initial for C1

Password Constitution	Number / Percentage	Common pattern identified
Begin with alphabets	321 / 84.5 %	Majority begin with small caps
Begin with number	13 / 3.4 %	Number '1' is the common number
Begin with special character	46 / 12.1 %	Character '@' is the common char
Total	**380**	

When creating and composing passwords for C1, it can be reported that thirteen participants of Science background and eleven participants of Islamic background composed their passwords with less than eight characters, albeit they were told not to do it. With regards to C2, it is found that seventeen participants composed their passwords with less than three words and hundred and five participants created their passwords with more than three words. Further analyses were conducted and found ten participants out of seventeen were actually composed their password using three words, but combined in one single word. Table 3 presents the C1 when they began to compose their passwords.

Having analysed the password memorability in previous sections, the followings are identified mistakes done by participants while participated in the second trial. The shared findings are general and not specific to three tested conditions.

a) The use of special characters. Participants were identified to use '*@ with a*', '*! with 1*', '*& with @*', '*$ with* ' and '*space with _*'.
b) Between conditions. Participants confused which password belongs to which condition.
c) In the case of password consists more than two words, participants normally confuse which one they use first. For example '*saya suka kamu*' is written as '*kamu suka saya*', '*AYAH IBU ANAK*' with '*IBU AYAH ANAK*', '*suka myvi dan viva*' with '*suka viva and myv*' and '*MEKAH is my birthplace*' with '*my birthplace is MEKAH*'.
d) The same word is interpreted differently. For instance, if participant used '*saya*', they changed to '*aku*' and '*kamu*' to '*awak*'.
e) In the case of password contains both word and number, it was identified that number of participants who normally forgot the number were higher as compared to word.
f) There exist participants who created their passwords based on colour (i.e. 'Red Apple' and 'Merah-merah delima'). It was found that participants forgot their chosen colour, but the frequency of occurrences is minimal.

In term of pattern during password creation, there are many but interesting patterns that can be reported are as follows:

a) Identified variation on the use of 'password' as the password are '*p4$word*', '*p@ssword8*' and '*pa$$word*'.
b) The use of password related to food is the most likely preferred and local foods such as '*teh tarik*', '*milo tabuh*', '*roti kosong*', '*nasi bujang*' are the most common occurrences.

c) Sequence of story. For example, C3 was made up from the combination of C1 and C2 respectively.

d) The uses of footballers name were obvious as well. For instance, '*messi*', '*ronaldo*', '*apek*', and '*farizal marlias*'.

e) Although participants do not directly use their actual name, but other clues could expose to password guessing. Examples like '*s-h-a-h-i-d-a@91*', '*D@rT2991*' and '*R@y@080890*'.

f) Most of the words created are in Bahasa Melayu, but there exist few occurrences of dialect words, distributed equally across peninsular Malaysia.

g) Same meaning, but with different phrase. Examples like '*saya sayang ummi*' with '*I love mummy*'; '*Aku sayang Allah*' with '*I love Allah*' and '*I don't know*' with '*I tak tahu*'

h) Repetitive occurrences of password for C2. Examples are '*saya suka awak*'(7 occurrences); '*saya suka makan*'(5 occurrences); '*I like it*' (3 occurrences); and '*nama saya ashraff*'(2 occurrences).

From the conduct of this analysis, authors acknowledged that participants of Science background were actually good at composing their passwords across all conditions, but unfortunately their levels of memorability were underperformed (i.e. this is just our honest thought but to verify what we have claimed, a statistical test is needed). On the other hand, although participants of Islamic background had good memorability, their composition of passwords were not as good as Science students as they created passwords related to Islamic or religious things and words related to their everyday life as students. These habits will result in insecure user behaviour and making password vulnerable to guessing.

4.3 Password Perception

In the feedback questionnaire, participants were asked to rate their perception towards level of difficulty when creating passwords and their perception on memorability of the created passwords. From Figure 3 (based on trial one), it can be reported that nearly 49% participants felt that C1 password is easy or somewhat easy to create, with 45% and only 17% participants rated C2 and C3 are easy or somewhat easy to create respectively. On the contrary, nearly 58% participants rated C3 was difficult, with C2 and C1 scored 17% and 26% respectively. Figure 3 also reported interesting finding as nearly 37% of participants' responded that password creation for C2 is neither easy nor difficult. Here, authors argue that the rating is having a direct relationship with the way participants created their passwords. Until no statistical test is conducted, our claim cannot be validated.

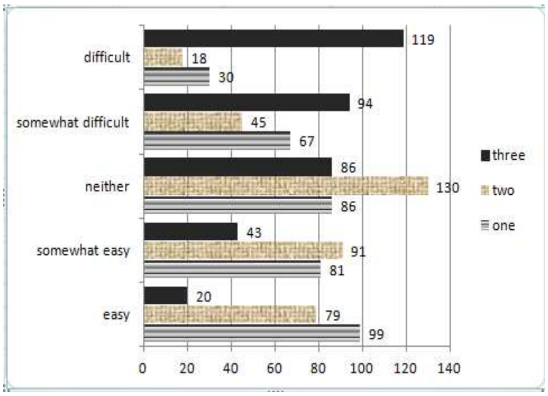

Figure 3: Participants' Perception towards Password Creation

As displayed in Figure 4 (based on trial two), 48% of participants felt that C1 password is easy or somewhat easy to remember, with 28% and 24% of participants rated C1 password as difficult or somewhat difficult and neutral (i.e. unsure) to remember respectively. In the C2, it can be divulged that 46% of participants rated easy, with 25% and 29% of participants rated 'not taking sides' or neutral and difficult respectively. Only 29% of participants rated C3 as easy, with nearly 44% and 27% participants rated difficult and neutral respectively.

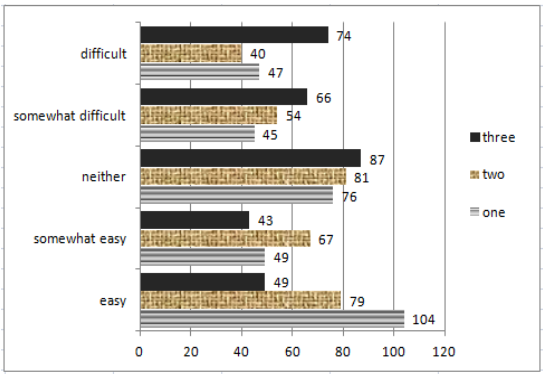

Figure 4: Participants' Perception towards Password Memorability

Another interesting finding which can be further explored is the percentage of participants who chosen 'neither easy nor difficult' across three conditions is most likely comparable. Comparing these finding with the aforementioned results reported previously, authors have a strong thought that there exist a direct relationship between password memorability with the password opinion upon memorability, despite no statistical analyses were made.

With respect to participants' password condition preference, Figure 5 clearly shows that for both trials, participants preferred C1 over others. The finding is quite interesting due to the fact that results reported in previous sections are not indicating any superiority of C1 over others. However, it can be suggested that participants had high awareness towards creating secure passwords.

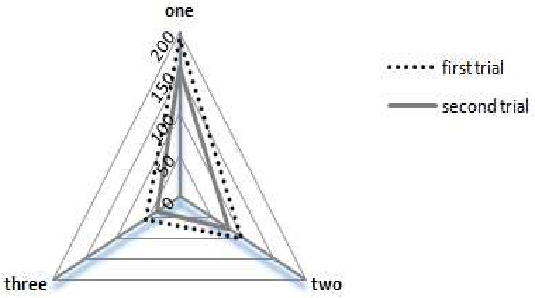

Figure 5: Participants' Preference towards Condition Choices.

With respect to reporting participants' opinion, authors revealed that numbers of participants are not equal and imbalance. This due to the fact that participants opted not to answer the feedback questionnaire, participants were absent when the trials were conducted, and there exist participants who only answered half of the feedback questionnaire. Having said this, it is still argued that results are still useful to indicate participants' preference towards three conditions, although not representative.

4.4 Lesson Learned

Having conducted the trial and analysed plain passwords from three categories, there are many lessons that authors have learnt. Overall, conducting this type of study within the larger population is fairly trade-offs as password created would not reflect their original daily use passwords. However, authors argue that the created passwords could be used for indication and prediction. From the analysis of results, it can be suggested that participants performed better (i.e. in term of their ability to remember) in C2, which directly suggest that participants still prefer using phrase or word. The result also reveals combining word with number will result in error during authentication.

As the participants were students, authors tend to agree that the reported results are predictive. For example, they have chosen typical passwords which directly associated with them such as daily intake foods, their interest in football teams and footballers name, song titles, artists and the way they composed their passwords (i.e. using their own dialect to voice out their origin and meaning of the word itself). These findings suggest that password prediction and guessing are possible, and it will be authors' critical agenda in the near future.

From the authors' point of view, although C1 and C3 look promising, however it can be suggested that the C2 is an ideal solution for complementing current password shortcomings. This due to the fact that C2 is believed could offer significant safety, and most importantly it could uphold users' memorability. In order to implement C2, it is suggested that common and guessable words should be avoided (as discussed earlier), between three to five words could be used and the composed passwords should be varies.

Results and findings within this trial echoes with other results from prior studies, regardless on the way it was conducted. Having said this, authors argue that it is not about the passwords itself; it is also the matter of users' habit when creating passwords, which directly expose them to threads and vulnerabilities. To control and safeguard users' insecure behaviour, the method like two factor authentication was proposed. This approach is getting popular as it currently being implemented by organisations such as Twitter, Facebook, LinkedIn, Google and Apple. Nevertheless, it could result in danger and problematic if the device is stolen, lost or compromised.

To reduce and safeguard users' burden of remembering many, long and complex passwords, mechanisms such as using password manager and single-sign-on (SSO) were proposed. However, if the main master passwords crack, the whole chains are compromised. The combination of smart card and biometric (i.e. from Omar et al., [29]) is another option and nowadays gaining much attention but this type of authentication is beyond the scope of knowledge-based authentication. Another interesting mechanism was based on the use of images/pictures (i.e. graphical passwords), claiming users are better in recognising and memorising series of images as compared to texts or phrases. However, from the conduct of research related to graphical passwords in [30] and [31]; outcomes were far than what should be expected.

5. CONCLUSION

This paper reports a study conducted to obtain users password based upon three conditions; password should contains a combination of upper case, lower case, number and special characters (C1), password should be created with a minimum number of three words (C2) and password should be created using two previous conditions (C3). Data collections were obtained from the authors' institution targeted from students with Islamic and Science background. Data were analysed and reported in three main criteria; namely password memorability, password creation and password perceptions. The study managed to recruit 380 students, having a total of 1140 plain passwords.

From the analysis, it can be reported that although they perceived these three conditions as secure and memorable, however common mistakes made by participants across three conditions are that participants tend to forget the actual special characters as well as their location. In addition, participants have problem to memorise the exact passwords, confuse from one condition to another, forget whether they had used upper or small caps and interestingly for C1 and C3, participants used different word for the second attempt, which actually having similar meaning with the first attempt. In term of password pattern, it could be exposed that participants do create patterns (i.e. footballer names, foods and beverages and sequence of story) when creating their passwords.

Although the analysis only reports on the surface level and no statistical tests were conducted for validation, it can be suggested that results reported within this paper are similar with previous results from other researchers regardless of age, culture, religious, and others. Current works is developing a Malay-based dictionary password for cracking purposes and extend the study to other institutions for having summative rather than predictive results.

Acknowledgement
Authors of this paper would like to thank all participants who participated and contributed to the findings. This work is funded by USIM under the internal research grant '*USIM Greenshoot Grant – PPP/GS/FST/SKTS/30/10812*'.

REFRENCES:

[1] RFC 2828. Authentication Definition, *IETF Reference Document*, Retrieved from http://www.ietf.org/rfc/rfc2828.txt., 2006.

[2] Vemuri, L. R., *What Is Authentication?* Retrieved from http://www.theiia.org/intauditor/itaudit/archives/2007/may/what-is-authentication, 2007.

[3] Liao, I., Lee, C., & Hwang, M., A password authentication scheme over insecure networks, *Journal of Computer and System Sciences*, 72, 727–740, 2006.

[4] O'Gorman, L., Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12), 2019 – 2040, 2003.

[5] Morris, R. & Thompson, K., Password security: a case history. *Communications of the ACM*, 22 (11) 594-597, 1979.

[6] Klein, D. V., Foiling the Cracker: A survey of, and improvement to, password security. In *Proceedings of the second (USENIX) Workshop on Security*. 5-14, 1990.

[7] Bishop, M., & Klein, D.V., Improving system security via protective password checking. *Computer & Security,* 14(3), 233-249, 1995.

[8] Adams, A., Sasse, M. A. & Lunt, P., Making passwords secure and usable. *Proceedings of HCI on People and Computers XII*. Springer-Verlag, 1-19, 1997.

[9] Carstens, D. S., McCauley-Bell, P. R., Malone, L. C. & DeMara, R. F., Evaluation of human impact of password authentication practices on information security. *Informing Science Journal*, 7 (1), 67-85, 2004.

[10] Schneier, B., *MySpace passwords aren't so dumb*. Retrieved on June 3, 2013 from http://www.wired.com/politics/security/commentary/securitymatters/2006/12/72300?currentPage=all, 2006.

[11] Florencio, D., & Herley, C., A large-scale study of web password habits. *Proceedings of the 16th International Conference on World Wide Web. Banff*, Alberta, Canada ACM New York, USA, 657-666, 2007.

[12] Bonneau, J., & Preibusch, S., The password thicket: technical and market failures in human authentication on the web. *The 9th Workshop on the Economics of Information Security (WEIS 2010)*. Harvard University, USA: June 7-8, 2010.

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

[14] Yan, J., Blackwell, A., Anderson, A., & Grant, A., Password memorability and security: empirical results. *Security & Privacy*, IEEE, 2004. 2(5): 25-31, 2004.

[15] Shay, R., Komanduri, S., Kelley, P.G., Leon, P.G., Mazurek, M.L., Bauer, L., Christin, N., & Cranor, L.F., Encountering stronger password requirements: user attitudes and behaviours. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*: ACM, 2010.

[16] Ur, B., Kelley, G.K., 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. In *Proc. USENIX Security*, 2012.

[17] Malone, D. & Maher, K., Investigating the distribution of password choices. In *Proceedings of the 21st international conference on World Wide Web*: ACM, 2011.

[18] Raza, M., Iqbal, M., Sharif, M., & Haider, W., A survey of password attacks and comparative analysis on methods for secure authentication. *World Applied Sciences Journal*, 19(4): 439-444, 2012.

[19] Jones, A. K., Password authentication with insecure communication, *Communications of the ACM*, 24 (11), 770 – 772, 1981.

[20] Bellovin, S.M., & Merritt, M., Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise. In *Proceedings of the 1st ACM conference on Computer and communications security*: ACM, 1993.

[21] Katz, J., R. Ostrovsky, & Yung, M., Efficient password-authenticated key exchange using human-memorable passwords, in *Advances in Cryptology, EUROCRYPT 2001*. Springer, 475-494, 2001.

[22] Gennaro, R., & Lindell, Y., A framework for password-based authenticated key exchange, in *Advances in Cryptology, EUROCRYPT 2003*. Springer, 524-543, 2003.

[23] Hafizul Islam, S. & Biswas, G., Design of improved password authentication and update scheme based on elliptic curve cryptography. *Mathematical and Computer Modelling 2011*.

[24] Chang, C., & Lee, J., An efficient and secure remote authentication scheme using smart cards, *An International Journal of Information & Security*, 18, 122-133, 2006.

[25] Das, M. L., Flexible and secure remote systems authentication scheme using smart cards, *HIT Transaction on ECCN*, 1 (2), 78-82, 2006.

[26] Ramasamy, R. & Muniyandi, A. P., An Efficient password authentication scheme for smart card, *International Journal of Network Security,* 14(3), 180-186, 2012.

[27] Klenk, A., Kinkelin, H., Eunicke, C., & Carle, G., Preventing identity theft with electronic identity cards and the trusted platform module. In *Proceedings of the Second European Workshop on System Security*, ACM., 2009/

[28] Baekdal, T., *The usability of password*. Retrieved from http://www.baekdal.com/insights/password-security-usability., 2007.

[29] Omar, M.H., Din, R., & Tahir H.M., Smart cards and the fingerprint: A framework for user identification and authentication. *Journal of Information and Communication Technology*, 2(1). 67-80, 2003.

[30] Chiasson, S., Usable authentication and click-based graphical password. *PhD Thesis*. School of Computer Science, Carleton University, Ottawa, Canada, 2008.

[31] English, R., Modelling the security of recognition-based graphical password schemes. *PhD Thesis*. School of Computing Science, Glasgow University, United Kingdom, 2012.