UTILIZING PERSUASION APPROACH TO IMPROVE COMPLIANCE BEHAVIOUR WITH PASSWORD GUIDELINES

Nur Haryani Zakaria

Universiti Utara Malaysia, Malaysia, haryani@uum.edu.my

ABSTRACT. Password based authentication remains the most commonly used authentication mechanism, in spite of the rapid introduction of several other authentication mechanisms such as smart cards, graphical passwords and biometrics. Users mainly rely on password guidelines to construct their password; nevertheless existing password guidelines seem inadequate especially from the perspective of influencing the users' security compliance behavior. Thus, this study intended to investigate ways to improve the content of password guidelines through persuasion approach to increase the likelihood of compliance behavior. A control laboratory experiment was carried out and the results were critically discussed. The outcomes indicate promising findings that users can be persuaded to improve their security compliance behavior by including more persuasive elements in the password guidelines.

Keywords: password guidelines, compliance behavior, persuasion approach

INTRODUCTION

Typical end users rely on a set of rules known as password guidelines, to which users must adhere when choosing a password. A password guideline mainly contains specific requirements on how a password should be composed. For example, the password must contain a minimum number of characters that must include uppercase letters or numbers and should not include words from the dictionary. There exist various types of password guidelines; however, there is consensus in the literature that well written password guidelines can provide increased security to the organizations (Campbell, Kleeman & Ma, 2006; Summer & Bosworth, 2004). It is posited here that password guidelines should include rationales as to why creating good (strong) passwords is important for users. Providing a rationale will increase the likelihood of compliance to a certain request (Cialdini, 2001).

This is especially lacking with the existing password guidelines, which focus more on providing information on how to compose a good password. Therefore, this study aims to investigate ways to improve the content of password guidelines. In conjunction with the inclusion of a rationale in the password guidelines, this study attempts to utilize two persuasion approaches: appeal strategy and two of the Cialdini's weapons of influence, to increase the likelihood of compliance. Generally, in order to guide this study, two research questions were formulated as follows; (1) Will users create better passwords when a rationale (i.e. an explanation of why creating good passwords is important) is included in the password guidelines? and (2) which persuasion strategies are more likely to result in influencing users to create better passwords?

The following section will briefly discuss some related work, research methodology along with the procedures of the experimental work involved. Results and analysis will then presented followed by an interesting discussion, conclusion as well as future work.

RELATED WORK

There are only few studies that have focused on the construction of password guidelines. As pointed out by Komanduri et al. (2011), there is lack of empirical data on passwords and the guidelines under which they were created. For instance, the NIST guidelines (Burr, Dodson & Polk, 2006) which are used to design password composition policies are based on theoretical estimates, while several other guidelines, such as in Proctor et al. (2002) and Vu et al. (2007) are based on a very small-scale laboratory studies.

Nevertheless, the content of password guidelines is important in providing suggestions to users on how to carry out security tasks such as creating good passwords. Besides the above studies, Grawmeyer and Johnson (2011) further investigated users' password generation behavior and revealed that users failed to interpret the contents of security guidelines given to them. Based on these several finding, authors draw a conclusion to suggest that password guidelines contained in security policies should be devised in order to avoid misconception among users.

Findings from existing studies seem to indicate that users are not convinced that such suggestions given in the guidelines are extremely important. This was indirectly pointed out in study by Shay et al. (2010), where, in spite of users' awareness, they were not deterred from continuing password practice that might put them at risk such as using dictionary words and names as well as sharing and reusing passwords. This study also confirms findings from previous studies (Wessels & Steenkamp, 2007; Zezschwitz et al. 2013) where users were also found to practice poor password habits, such as using names and birth dates to construct their passwords and using the same password across multiple accounts.

RESEARCH METHODOLOGY

A controlled laboratory experiment was carried out to investigate the research questions of this study. The experiment used the between-subject design, where each participant is exposed to only one of the experimental conditions. There will be one control group (no inducement) and four experimental groups as follows; (1) Rational appeal group, (2) Emotional appeal group, (3) Social proof group and (4) Commitment & consistencies group (C&C).

The apparatus used in this experiment are as follows; the instructions set, the five password guidelines for the experimental groups (including the control group), a password login prototype, and a set of questionnaires. The instructions sets were uniform across all participants; everyone received the same instructions and was informed that the Information System & Services Department of the university wanted all the students to create a new login account to replace the existing one. The instructions were typed on a piece of paper with a slightly larger font (i.e. 16 font *Times New Roman*) to make it clear and readable to participants.

The password guideline sets which were distributed to the participants vary according to the group to which they were assigned. For example, the persuasive argument for the rational group was framed using logical reasoning by providing relevant examples such as the fact that the variety of usable characters in the passwords will significantly increase the difficulty in hacking the passwords. The persuasive argument for the emotional group was framed by attempting to invoke the participants' emotions; this was achieved by giving examples of real hacking incidents which resulted in the passwords being compromised due to weakness. The persuasive argument for the social proof group was framed by attempting to associate the participants with the current scenario of popular social networking sites (e.g. Facebook) where passwords being compromised could not only jeopardize important personal accounts but also reputation among friends as the hackers are able to take charge of their profile in the social networking sites. Slightly different from the first three experimental groups, the participants in the commitment and consistency group did not receive a persuasive argument informing them why creating a good password is important; instead, they received a recommendation statement to request them to create a strong password as it is very important to ensure compliance behavior is met. The participants in this group were then requested to formalize their agreement (i.e. to create strong password) by signing in the commitment page. Furthermore, the participants were told that the commitment page would be handed to and reviewed by the ISS departmental staff. Finally, the participants in the control group only received the standard NIST password guidelines similar to those received by the participants from other groups and nothing else. The last apparatus involved in the experiment is the set of questionnaires containing several questions on demographic details of the participants and also some questions related to password constructions and usage.

The measurements involved in the experiment are password strength and password compliance. The password strength was measured using a combination of several important attributes that constitute a particular password, such as length (i.e. characters), the frequency of uppercase, lowercase, alphabetic characters, numerical characters and alphanumeric characters (e.g.: @, #, !, etc.). A tool known as the "*Password Meter*" is adopted in this study to measure password strength (Password Meter, 2012). The password strength is calculated by adding points (+) if the password exhibits certain required attributes and deducting (-) points if the password fails to exhibit certain attributes. The score given is in the form of percentages, where the maximum will be 100%. The passwords will be categorized as weak, acceptable and strong according to the following scores; (≤ 30%), (30% ≤ x ≤ 60%) and (≥ 60%) respectively. Therefore, the required score to indicate the compliance level is 30 points following the metrics as anything below is considered weak password.

The next element that was also measured in this experiment is the password compliance. It is basically refers to how close each participant follows the requirements given in the password guidelines. Therefore, each requirement was allocated some points accordingly to indicate the total score of compliance for each of the password created by participants.

The experimental procedures

The experiment was conducted at one of the public university with various departments ranging from sciences to social sciences. The experiment was advertised through university websites after being approved by the University Ethics Committee (UEC) whereby interested participants sent email to express their willingness to participate.

To begin with, all participants were given a unique id number which automatically placed them randomly into one of the five experimental groups. They were given a brief introductory session to sign the consent form and supply demographic details. Following the experimental scenario, all participants were given a standard NIST password guideline. Participants were then asked to create a password for their university login account. Information on the frequency of character types that constitute each participant's invented password was collected. For example, if the password was p@ssword123, the data collected would have been: 7 lower case letters, 3 numbers, 1 special character and 11 as the length. The participants were requested to log in immediately after the account had been created. Finally, the participants were asked to fill in short questionnaires on some related to password construction usage. Participants signed the remuneration form before leaving the experimental room where each participant was rewarded a small token of souvenir for their time and effort in participating.

RESULTS & ANALYSIS

A total of 75 participants took part in the experiment, of which 31% were male. More than half of the participants (67%) who took part were aged between 18 – 25 years old, of whom about 75% were post-graduate students. The participants were almost equally divided in terms of technical and non-technical background; 49% and 51% respectively. The password created by all the participants from the five experimental groups will be examined according to several factors (i.e.: compliance, strength, length, unique characters used and number of different character sets) as summarized in Table 1 below.

Table 1. Mean and (standard deviation) of several password elements analyzed according to the five experimental groups

Groups/ Passwords Factors	**Password Strength**	**Password Compliance**	**Length**	**Unique Characters Used**	**Number of Different Character Sets**
Rational	79.93 (18.39)	32.87 (4.03)	9.80 (1.52)	8.40 (1.29)	3.40 (0.63)
Emotional	85.67 (17.01)	35.0 (4.80)	10.33 (1.99)	8.33 (1.68)	3.53 (0.63)
Social proof	85.80 (19.80)	33.93 (3.73)	11.27 (2.63)	8.87 (2.03)	3.13 (0.52)
Commitment & Consistencies	74.33 (20.94)	31.73 (4.50)	10.40 (2.27)	8.40 (1.68)	2.87 (0.74)
Control	63.27 (27.85)	30.87 (5.96)	9.87 (1.92)	8.00 (1.85)	2.80 (1.01)

**In each cell – The mean of password factors scores followed by the standard deviation in brackets.*

Table 2. The results for One-way ANOVA of all the password elements analyzed

Groups/ Passwords Factors	**Password Score**	**Password Compliance**	**Length**	**Unique Characters Used**	**Number of Different Character Sets**
One-way ANOVA	F=2.97, **p-value=0.025**	F=1.89, p-value=0.12	F=1.24 p-value=0.30	F=0.48 p-value=0.749	F=2.91 **p-value=0.027**

**The items in bold shows the p-value for statistically significant difference detected*

Meanwhile, Table 2 reports on the One-way ANOVA test on all the password elements analyzed. The results of password compliance have shown that all the experimental groups including the control group have reached the mean compliance score above 30 points which indicates that in general majority of the participants in this experiment have complied with the requirements given in the password guidelines. This can be seen from Table 1 whereby the highest compliance mean score was seen to be coming from the emotional group (35.0) followed by the social proof group (33.93) while the lowest mean score comes from the control group (30.87). However, there was no significance difference detected with One-way ANOVA test (F=1.89, p-value=0.12) which seems to indicate that the persuasion strategies applied did not have much of an effect on compliance level among participants in this study.

Looking further into the passwords created by the participants, the results of their password strength have shown that the social proof group has the highest mean (85.80) followed by the emotional group (85.67), with the lowest being the control group (63.27). The results were further analyzed using One-way ANOVA and the results reveal a significant difference across the five conditions (F=2.97, p-value=0.025). This indicates that participants create stronger passwords when they receive guidelines with persuasive rationales, compared to passwords without persuasive rationales included in the guidelines. However, further tests are required to identify which of the various approaches applied is the most effective. A Tukey post hoc test was conducted to examine this question. The Tukey test revealed with 95% confidence intervals, that the social proof and emotional groups are significantly different from the rest of the groups, indicating that more participants are persuaded with these two approaches compared to the others.

Moreover, the passwords constructed by the participants from the social proof and emotional groups, 67% of both groups had passwords that were categorized as very strong passwords (password score ≥ 80%). However, participants in the social proof group constructed much better passwords than the emotional group when comparing each element that contributed to the password score (i.e. length, unique characters used, number of different character sets). As can be seen from Table 1 above, the mean for all the elements mentioned above was higher for the social proof group compared to the emotional group. Moreover, approximately 40% of passwords constructed in the social proof group had a perfect score (i.e. 100%) compared to only 27% in the emotional group.

The One-Way ANOVA test was also conducted towards other password elements as well as reported in Table 2 above. Based on the results displayed on that table, two elements of the passwords which are length and unique characters used indicated no significant difference – however, there was a statistically significant difference detected for the number of different characters sets used by the participants to construct their password which indicates a supporting factors for the significant effect detected in the password strength.

DISCUSSION

The control-laboratory experiment conducted has yielded results as presented in previous sections. At the beginning of the experiment, several research questions were formulated. In this section, those research questions will be revisited and discussed. The first question asked whether users would create better passwords when a rationale explaining why creating a good password is important is included in the password guidelines. The results indicate that passwords created by users who receive password guidelines including a rationale are stronger compared to passwords created by those who did not. The results of password compliance seem to be consistent with the passwords strength constructed.

Thus, these findings suggest that it is worth providing extra information to users on why such task as creating a good password is important. However, the challenge is to ensure that users will make an effort to read this information, as that which is depicted in the control-laboratory experiment might not happen in the real world. However, one possible way to overcome this is to include reading and understanding the password guidelines as a compulsory phase before someone could actually construct a password. This is especially worth considering if the systems or applications require a high level of password security.

The second question focused on which persuasion strategies are more likely to result in influencing users to create better passwords. The results show that participants who are exposed to the emotional appeal and social proof strategies produce stronger passwords than the others. These two strategies are probably more effective than the others as the explanations provided in the strategy easily relate to the participants (i.e. the emotional appeal uses a real life scenario) and social proof endorsement is probably very important to them. On the other hand, participants in the commitment & consistency group were found not to produce passwords as strong as the other experimental group, probably due to the fact that this strategy might not work so well in the experimental setting but might yield better performance in a real world scenario. This is because the impact portrayed by the surveillance factor is important to ensure this strategy works; otherwise, the audience might not be immersed in the effect of noncompliance.

CONCLUSION & FUTURE WORK

This article has presented the control-laboratory experiment conducted to evaluate the study of persuasion and individual behavior in constructing passwords. While motivating users' security compliance through persuasion is practical for the password authentication domain, there is a more fundamental problem in this domain that needs addressing – namely the problem of memorability. Most people are found to cope with memory overload by relying on one or two obvious passwords (e.g.: birth dates or combination of partner's name) but unfortunately although these weak passwords tend to ease the overload problem but they fail to offer adequate levels of protection (Briggs & Oliver, 2008). Therefore, in the next part of the study is to focus towards looking into alternative countermeasures which may help solve the memorability problem.

REFERENCES

Briggs, P. & Olivier, P. (2008). Biometric Daemons: Authentication via Electronic Pets. In Proceedings of *The Conference on Human Factors in Computing Systems (CHI'08),* Florence, Italy, April 5 – 10, 2008, USENIX Association Berkeley, CA, 2423-2432.

Burr, W. E., Dodson, D. F., & Polk, W. T. (2006). *Electronic Authentication Guideline*. National Institute of Standards and Technology.

Campbell, J., Ma, W., & Kleeman, D. (2006). Password Composition Policy: Does Enforcement Lead to Better Password Choices. In Proceedings of *The 17th Australian Conference on Information Systems*, Adelaide, Australia, December 6 – 8, Australian Association for Information System, 60 – 69.

Cialdini, R. B. (2001). Harnessing the Science of Persuasion. *Harvard Business Review*, 72-79.

Grawmeyer, B., & Johnson, H. (2011). Using Multiple Password: A Week to a View. *Interacting With Computers*, *23*(3) 256-267.

Komanduri, S., Shay, R., Kelly, P. G., Mazurek, M. L., Bauer, L., Christin, N., . . . Egelman, S. (2011). Of Passwords and People: Measuring the Effect of Password-Composition Policies. In Proceedings of *The Human Factors and Computing Systems*, Vancouver, BC, Canada, May 7 – 12, 2011, ACMPress New York, NY, USA, 2595-2604.

Proctor, R. W., Lien, M. C., Vu, K. P. L., & Schultz, E. E. (2002). Improving Computer Security for Authentication of Users: Influence of Proactive Password Restrictions. *Behaviour Res. Methods, Instruments & Computers*, *34*, 163-169.

Shay, R., Komanduri, S., Kelly, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., . . . Cranor, L. F. (2010). Encountering Stronger Password Requirements: User Attitudes and Behaviours. In Proceedings of *The Symposium on Usable Privacy and Security (SOUPS'10)*, Redmond, WA, USA, ACMPress, New York, NY, USA, July 14 – 16, 2010, 14 – 34.

Summers, W. C., & Bosworth, E. (2004). Password Policy; The Good, The Bad and The Ugly. In Proceedings of *The Winter International Symposium on Information and Communication Technologies*, Cancun, Mexico, January 5 – 8, 2004, ACMPress New York, NY, USA, 1- 6.

The Password Meter (n.d). Retrieved May, 12, 2012, from http://www.passwordmeter.com/

Vu, K. P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B. L. B., & Cook, J. (2007). Improving Password Security and Memorability to Protect Personal and Organisational Information. *International Journal of Human-Comp. Studies, 65*, 744-757.

Wessels, P. L., & Steenkamp, L. P. (2007). Assessment of Current Practices in Creating and Using Passwords as a Control Mechanism for Information Access. *South African Journal of Information Management, 9*, 1-14.

Zezschwitz, E. V., De Luca, A. & Hussmann, H. (2013). Survival of the Shortest: A Retrospective Analysis of Influencing Factors on Password Composition. *INTERACT 2013*, Part III, LNCS 8119, 460–467.