2nd International Conference on Information and Communication Technology and Its Applications (ICTA 2018)
Federal University of Technology, Minna, Nigeria
September 5 – 6, 2018

Effect of Mental State and Personality on Password Selection Among Mobile Phone Users: A Case Study of IBB University Lapai Students

Abdullahi Abubakar Kawu[1], Idris Muhammad[2], Aisha Awal[3], and Muhammad Bashir Abdullahi[4]
[1, 2, 3]Department of Computer Science, Ibrahim Badamasi Babangida University, Lapai, Nigeria
[4]Department of Computer Science, Federal University of Technology, Minna, Nigeria
{[1]abdullahikawu, [3]aishaa}@ibbul.edu.ng, [2]mail4idris@gmail.com, [4]el.bashir02@futminna.edu.ng

***Abstract*—There is a paucity of research that examine the psychological state of mobile phone users while creating passwords, and how it affects the choice of strong and weak passwords. In this paper, we examine how a user's mental state and personality affects choice of user's password. Therefore, we use two groups: experimental and control, each of 16 subjects, who were asked to generate a password. At the beginning, all participants used the BMIS and the BFI tools to self-report their mental state of mind and personality, respectively. Then, we exert mental fatigue on participants in the experimental group while those of other group were not. At the end of the experiment, we measure and compare password strength across groups. Our findings reveal that the effect of the different mental states on password over our limited sample size is not so different, although more mentally fatigued users tend to create weaker passwords than others do. Further, we demonstrate that a relationship exists, nonetheless, as indicated by our regression model. We also investigated personality and its implication on password strength, the study reveals that participants who report as agreeable are more likely to create better passwords than conscientious participants or extraverts.**

Keywords: password; ubiquitious security; personality trait; HCI

I. INTRODUCTION

Users have a responsibility to create strong passwords for computing systems, but they often failed due to various reasons such as tendency to set easy to remember passwords, avoidance of complexity or overload that might arise from remembering different passwords for different services. Thus, there is a significant amount of researches on user behavior with password that examine how they manage passwords [1], and how security systems have failed to consider user dynamics [2]. However, only few studies consider psychological state and activities that contributes to how users formed their passwords.

Gross *et al*., [3] study the effect of personality, mood and cognition on password strength. However, the study only considered users of a typical computing system such as personal computer (Laptop) or the desktop systems. Nowadays, many users leverage on portability of mobile phones or smartphones to transact daily businesses and storage of sensitive data. Thus, users need to create, use and appropriate passwords on their portable devices.

Furthermore, most services have peculiar layout for each platform: mobile phones and desktop computer views, respectively. Hence, in this paper, we investigate the effect of mental state otherwise referred to as cognition and personality on password choices of mobile phone users.

The rest of this paper is organized as follows. In Section II, we discuss the related work. Section III describes the methodology used for investigation. In Section IV, we demonstrate the results obtained by performing experiments in simulation. Lastly, we present concluding remarks in Section V.

II. RELATED WORK

Password-based approaches remain the prevalent way of user authentication despite the many sophisticated and viable security alternatives that have emerged from research and development [4]. It is largely adopted due to its cheapness to both security providers and users. Research on password has focused largely on how users cope with the multitude of challenges pose by management of the password such as memorability, re-use, and password aids (password cues, meters, password managers) [3].

A. Password Management Practices of Users

Studies show that passwords are often compromised through the poor security and management practices of users [1, 4]. Passwords are supposed to be secrets, shared only between the user and the system for authentication. However, users have proven repeatedly that they are not able to accomplish safely the responsibilities of keeping these secrets especially in the face of multiplicity [3]. Thus, they result to keep them in unacceptable ways; they write them down [1], or in discrete cases they even tell friends and close family members believing that it is safe with them too [5]. The study by [1] presents interesting findings about how users manage their passwords. The authors explained further on how users failed in meeting security objectives and what behaviors they adopt in those circumstances. Additionally, the authors reported the burden of living with passwords and users' workaround or strategies to alleviate those burdens.

The use of password managers appeared to be one of the most effective ways to manage passwords. If well designed, and passwords not stored openly, password managers seem to offer one of the best solutions for password management: comprehensive, convenient, and safe. However, many typical users do not use password managers; they in fact do not understand what they meant, how they are used [1], when they are used. Consequently, Users find usability issues with password managers [1, 6].

B. Choice of Passwords

Password choice is a fundamental security research issue. An average user has 6.5 passwords, and each password can be shared across 3.9 different services [7]. Making choices across these services can be rather cumbersome, hence the need to find password improvement mechanism. Research and products have emerged in this direction [3, 5]. Some researches and products focused on the length, format and vulnerability of passwords [5]. Others have highlighted remedies that include graphical passwords [3], password checkers, password generators, password aging mechanisms and password managers [5]. In addition, complete alternatives to passwords exist in the form of biometrics and security tokens, but there are reported issues of privacy, theft and thus, present huge costs in deployment and maintenance of these alternatives [6]. However, majority of these alternatives do not account for the state of mind of users when creating them.

C. Mental State

Experts have agreed that security mechanisms are not to be looked at in isolation [5]. It is important that security professionals consider the socio-physical context of the security mechanism like the mental state of users. Mental state has mainly been studied in psychological, clinical or a few multi-disciplinary realms. It usually involves studies in extended periods with tasks that have to be carried out for at least two hours. Yet, it was shown in the literature on the loss of self-control that cognitive control could be impaired after short and simple attempts at self-control. Therefore, whenever an individual is engaging in cognitively challenging tasks for a long time could result to a state of mental fatigue, which has consequences as increased distractibility, impaired decision-making, or more generally an impairment of cognitive control processes [8, 9]. More so, the studies of mental fatigue have mostly applied to very easy tasks involving only a little amount of cognitive control but for extended periods. Conversely, the study by [9] proposed a shorter period of challenging tasks that can lead to mental fatigue.

In this study, we consider the above proposition made by [9] and thus use similar but extended manipulation tasks for inducing cognitive depletion as in [3] to achieve artificially induced mental fatigue user. Furthermore, we appropriated the use of the research outcomes from psychology to pervasive security setting. Examples of studies in this direction are the work of [1, 3]. In their work, Gross *et al*., [3] reported that cognitive depletion does affect password strength for a typical user of a computing system. However, the study employed only 10 Stroop task items for cognitive effort manipulation. In addition, only about 29% of participants in the study were reported to have been cognitively depleted successfully.

III. METHODOLOGY

A. Participants

The 32 subjects we used for the study were undergraduate students from IBB University, Lapai, Nigeria, which consist of 16 females and 16 males, aged between 18 and 35 years. They were motivated with a 50 Naira recharge card each in exchange for participation. We divided the participants into two groups: control and experimental groups. We tested all the participants individually. We kept the experimental group in a room for the entire session of the study and the control group is not.

B. Procedure

We set-up the experiment to compare the effect of mental fatigue on password strength of mobile users. To achieve this, we initially subjected the experimental group to mentally challenging tasks that could result to mental fatigue for 17 minutes. While the control group was not. Thereafter, both groups complete non-fatigue tasks with similar length and structure. The detailed procedure is as follow:

- Pre-task questionnaire detailing relevant demographic of each participant.
- A personality trait questionnaire to identify personality of each participant.
- Challenging manipulation tasks to induce mental fatigue of the experimental group.
- A manipulation check on the level of fatigue.
- A password entry for a mock-up mobile Gmail registration.

C. Personality Trait

We investigate personality trait as a covariate to mental fatigue using the Berkeley Big Five Inventory (BFI). We gave each participant a BFI questionnaire that reveals their personality using methodologies inspired by [10]. However, given the time constraints on the part of the participants, we sought for a shorter form of the tool, the 10-item BFI [11] and agreed to use three (3) traits out of the list of five (5) traits to evaluate. The three traits from BFI are Extraversion or Surgency (talkative, assertive, energetic), Agreeableness (good-natured, cooperative, trustful) and Conscientiousness (orderly, responsible, dependable).

D. Inducing Mental Fatigue

To induce mental fatigue, we leverage on the earlier work of Lerner *et al*., [12], Rauch & Schmitt [9], Gross *et al*. [3], and Wegner *et al*. [13]. In the experimental condition, participants were asked to suppress their thoughts, undertake Stroop tasks and watch emotionally inducing movie as the manipulation activities. In the control condition, the participants completed tasks with a similar length and structure. The following provide details of the manipulation activities.

1) Thought Suppression Tasks

In the experimental condition, the participants were shown a photo of a white bear and asked not to think of the white bear i.e supress the thought, following the procedure by Wegner *et al*. [13]. They were to raise their hand should they failed to suppress the thought. While in the control condition, the participants were asked to write Y indicating "Yes" whenever they think about the white bear but not instructed to suppress their thought. This activity lasted for 5minutes.

2) Stroop Tasks

These tasks were adapted from [5, 14] as fatigue inducing tasks. Two variants of the Stroop tasks were given to each participant, the numerical Stroop tasks and the conventional coloured word Stroop task. Stimuli (coloured words and numbers) were presented to participants on a printed paper, and they were asked to mention the colour in which each word was presented. We first provided 88 (Type A) congruent items (i.e. word and colour or number were the same) as a short practice session, before the actual trials, which involved 88 congruent items (Type B) and 60 - (Type C) incongruent items (i.e. word and colour were different). Figure 1 is a sample of Stroop task item. The Stroop condition is that the name of a colour (e.g., 'red') is printed in a colour not denoted by the name (incongruent colour and name).The experimental condition involved answering 176 items without the Stroop condition and 88 Stroop items with the Stroop condition (Type A, B & C). These tasks are mentally effortful when Stroop condition is achieved and it lasted for 10 minutes. The control condition participants answered only 176 items without the Stroop tasks (Type A & B).

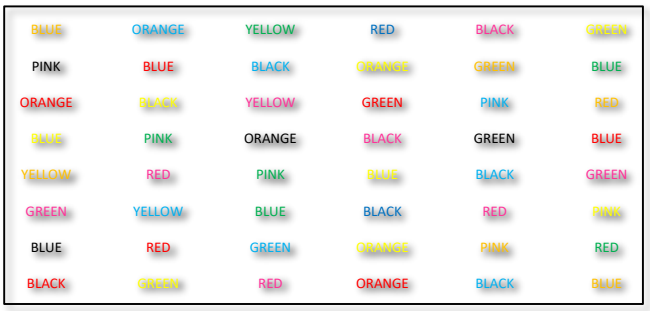

Figure 1. Sample Stroop task items

3) Emotion inducement task

This activity follows findings by Muraven et al [15]. They posit that emotional inducement and control impacts on cognition and subsequently contributes to mental fatigue. We adopted methods from [11, 16] to induce emotion. In the experimental group, participants were asked to watch a video clip that would induce sadness for 5 minutes. The scene of the video is about the death of a boy's mentor. In contrast, the control group participants were asked to watch a video clip of a documentary about nature, a fish in the Great Barrier Reef [16].

E. Manipulation Check on Mental Fatigue

Researches have suggested the use of the Positive and Negative Affect Schedule (PANAS) or Brief Mood Introspection Scale (BMIS) as a check tool for psychological experiments that involve cognition, mood, affect and mental fatigue [17, 18]. We chose to use the Adapted BMIS [17] owing to its simple wordings compared to PANAS [18]. Both the experimental group and the control group were given this tool to evaluate the mental state of each participants after the experiment.

F. Gmail Registration on Smartphone

Participants from both groups were asked to generate a new password for a Google Mail (GMail) on a mock-up GMail Android Application that was visually identical to a Gmail Registration screen on a mobile phone. This was the last task in the experiment and participant were requested to create a new GMail account. They were told it is very important and they should ensure they would remember the password at a later date. Registered username and password were recorded on the device.

G. Password Strength

The consensus definition of a password's strength is the number of attempts that an attacker would need in order to guess it [18]. There are various ways and state of the art products to test the strength of passwords like the use of Keepass, PGS or Dropbox's zxcvbn [19, 20] but we settled to use an online password meter [1] because it provides a quantitative value useful for comparison in addition to other features similar to the more acclaimed password meters. The password meter was used to evaluate the strength of the password of each participant in both experimental and control groups. We used both textual evaluation (weak, medium and strong) as well as the score as the metrics for our analysis.

IV. Results and Analysis

We employed two approaches to analyze the results. In the first approach, we used simple descriptive statistics to provide a lay explanation of what have happened. The Table I, Table II and column bar chart as shown in Figure 2 presented the results.

A. Password Strength and Mental state

TABLE I. Password Strenght vs Mental State

Mental State	**Password Strength**			
	N	***Weak***	***Medium***	***Strong***
Fatigued	10	9	1	0
Effortful	11	9	2	0
Not fatigued	11	9	2	0

The Table I shows that all participant created either a weak password or a sizeably medium strength passwords. Specifically, most fatigued participants (90%) created weaker password, compared to mildly fatigued (effortful) and not-

[1] www.passwordmeter.com

fatigued participants (about 82%) who also created weak passwords but at a slightly improved rate. Password score for all participants were recorded and were in the range between 14 and 53.

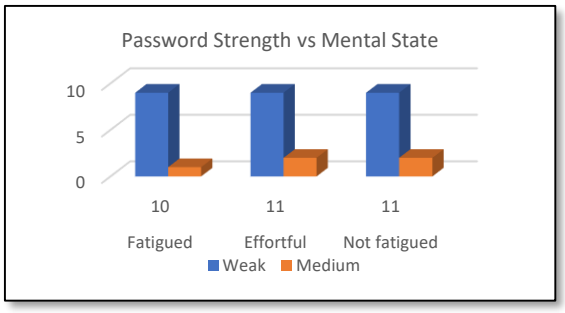

Figure 2. Password strenght and mental state

The password strength difference may not be as statistically significant in terms of number of participants as the score per participants considering the findings by [3]. Hence, our second approach.

In the second approach, we used multiple stepwise regression to explore correlation (relationship) or predictive tendencies of relative variables. In particular, we sought to explore the effect of gender, mental state, and personality trait on password strength. However, due to the small sample size, we projected (bootstrapped) the sample size to 96. As a result, we obtained an overall adjusted $R^2 = 0.43$ and a predictor of importance of 0.108 with $p = 0.24 > 0.05$ at 95% confidence interval. Consequently, the following variables were excluded in the final model; gender and personality trait, an outcome, which slightly differs from that of [3], except for gender, which was also found out to be a non-predictor of password strength in both studies. Our regression model can be represented by the equation:

$$P = 0.965 + 0.108m$$

where: P = Password Strength and m = Mental State.

It was observed that we were relatively successful in artificially inducing the mental state in some participants (31%), which is better than 29% in the study by [3].

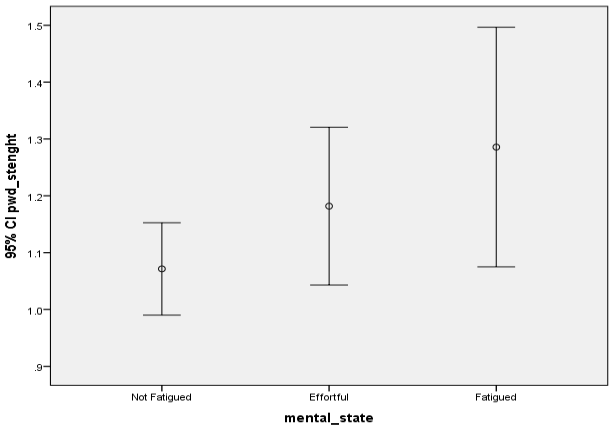

Figure 3. Password Strength by Mental State (Error bars 95CI)

B. *Password Strength and Personality Trait*

We also investigated how personality might impact on password strength. Table II shows the findings from our study.

TABLE II. PASSWORD STRENGHT VS PERSONALITY TRAIT

Personality	Password Strength		
	N	*Weak*	*Medium*
Extraversion	14	12	2
Agreeableness	12	9	3
Conscientiousness	6	6	0

All conscientious participants created weaker passwords similar to individuals who self-report as extraverts. However, ¼ of participants who reported as agreeable created better passwords compared to 1/7 of participants who reported as extraverts.

V. LIMITATIONS OF THE STUDY

A few limitations that could inspire and aid future researches are accounted below:

A. *Experiment condition or tasks*

The thought suppression task used in this study was not as effective as we thought; the use of the white bear was neither transparent to the experimenter nor was it easily understood by the participants. The other artificially induced mental fatigue tasks used seems more transparent and effective in this circumstance, hence future research could avoid the use of white bear task as a mental fatigue inducing task. Similarly, the experimenters observed that the use of colour words were more effective in creating a Stroop condition than a numerical Stroop variant we introduced as an addition. Another consideration in future research could be to investigate the effect of physical fatigue on password choice.

B. *Adapting research tools*

We gave the participants all the 16 dimensions in the adapted BMIS tool. However, a considerable amount of them does not understand the meaning of some words contrary to our expectations. The words grouchy, peppy, content, nervous were particularly problematic for most participants. Hence, future researches should consider appropriating the tool to words or adjectives the participants would be familiar with and relevant to the study as suggested by Gross *et al.* [3].

C. *Participants' Composition and sample size*

Most participants are young users between the age of 18 – 35 years. Study can investigate older users. We also require more people to participate to improve the quality of the sample size and consequently the result. Our participants are of African origin particularly Nigeria, other researches can consider participants from other nationalities.

D. *Patterns in Participants' Password*

We observed that the participants chose their passwords following a pattern. Many of them have used a combination of digits from their phone numbers (some excluding only the first zero - 'O'), which makes them highly susceptible to

varying attacks (guessing attack especially). Future studies can investigate this further.

VI. CONCLUSION

This study reveals that there is a nexus between a user's mental state and their chosen password. Thus, it shows that a stable mental state is necessary for the creation of stronger passwords. Mentally fatigued users created weaker passwords than mildly fatigued users (effortful) and non-fatigued users. Furthermore, a linear regression showed that mental state can predict password strength with an overall adjusted $R^2 = 0.43$ and a predictor of importance of 0.108 with $p = 0.24$. Our results are indicative and validate the importance of user's mental state in security. In addition, our findings suggest the need for interesting design paradigms for password-based systems and HCI interventions to support the user's password creation process such as replicating the use of adaptive and emotion induced interfaces as is obtainable in search engines, notably Google search. It also provides useful information towards a review of existing password security policies such as 'be mentally alert to have a better password' or 'do not create a password while mentally tired'.

ACKNOWLEDGMENT

We want to thank colleagues from IBBU University, Department of Mathematics and Department of Computer Science for their inputs into this research. In particular, the effort of Mrs Amina Abbas and Dr. Ayodele Agboluaje for his review of relevant statistical data is highly appreciated. We are also grateful to our volunteers who spared time to participate in this research.

REFERENCES

[1] E. Stobert and R. Biddle, "The password life cycle: user behavior in managing passwords" In Proceedings of Tenth Symposium on Usable Privacy and Security (SOUPS), pp. 243-255, 2014.

[2] A. Adams and M. A. Sasse, "Users are not the enemy" Communications of the ACM, vol. 42, issue 12, pp. 40-46, 1999.

[3] T. Gross, K. P. Coopamootoo and A. Al-Jabri, "Effect of Cognitive Effort on Password Choice", In proceedings of Learning from Authoritative Security Experiment Results Workshop (LASER) pp. 55-66, 2016.

[4] K. Bryant and J. Campbell, "User Behaviours Associated with Password Security and Management", Australasian Journal of Information Systems, vol. 14, no. 1, pp. 81-100, 2006.

[5] D. Gollmann, "Computer security", Wiley Interdisciplinary Reviews: Computational Statistics, vol. 2, no. 5, pp.544-554, 2006.

[6] S. Chiasson, P. C. Van Oorschot, and R. Biddle, "A usability study and critique of two password managers", In proceedings of the 15th USENIX Security Symposium, vol. 15, pp. 1–16, 2006.

[7] D. Florencio and C. Herlye, "A large-scale study of web password habits", In proceedings of the 16th International Conference on World Wide Web (WWW '07), pp. 657-666, 2007.

[8] L. R. Hartley, F. Penna, A. Corry and A. M. Feyer, "Comprehensive review of fatigue research", Murdoch University. Institute for Research in Safety & Transport, 1997.

[9] W. Rauch and K. Schmitt, "Fatigue of cognitive control in the stroop-task", In Proceedings of the Annual Meeting of the Cognitive Science Society, vol. 31, no. 31, pp. 750-755, 2009.

[10] O. P. John and S. Srivastava, "The Big-Five trait taxonomy: History, measurement, and theoretical perspectives", In L. A. Pervin and O. P. John (Eds.), Handbook of personality: Theory and research, Vol. 2, pp. 102–138, 1999. New York: Guilford Press.

[11] B. Rammstedt and O. P. John, "Measuring personality in one minute or less: A 10-item short version of the Big Five Inventory in English and German", Journal of Research in Personality, vol. 41, pp. 203-212, 2007.

[12] J. S. Lerner, D. A. Small and G. Lowenstein, "Heart strings and purse strings: Carryover Effects of emotions on economic decisions", Psychological Science, vol. 15, pp. 337-341, 2004.

[13] D. M. Wegner, D. J. Schneider, S. R. Carter and T. L. White, "Paradoxical effects of thought suppression", Journal of personality and social psychology, vol. 53, no. 1, p.5-13, 1987.

[14] C. M. MacLeod, "The Stroop Effect", Encyclopedia of Color Science and Technology 2015. DOI 10.1007/978-3-642-27851-8_67-1.

[15] M. Muraven, D. M. Tice and R. F. Baumeister, "Self-control as a limited resource: Regulatory depletion patterns", Journal of Personality and Social Psychology, 74, pp 774 – 789, 1998.

[16] JoVE, Cambridge, MA, JoVE Science Education Database. Social Psychology. Inducing Emotions retrieved from https://www.jove.com/science-education/10308/inducing -emotions. 2018.

[17] R. F. Baumeister, K. D. Vohs and D. M. Tice, "The strength model of self-control", Current directions in psychological science, vol. 16, no. 6, pp. 351–355, 2007.

[18] D. Watson, L. A. Clark and A. Tellegan, "Development and validation of brief measures of positive and negative affect: The PANAS scales", Journal of Personality and Social Psychology, vol. 54, no. 6, pp. 1063-1070, 1998.

[19] D. L. Wheeler, "zxcvbn: Low-Budget Password Strength Estimation", In proceedings of the 25th USENIX Security Symposium, pp. 157-173, 2016.

[20] KeePass Help Center: Password Quality Estimation. Retrieved from http://keepass.info/ help/kb/pw_quality_est.html. 2018.