A Peer Pressure Method for Helping End-Users Generate Strong Passwords

[1]S. Agholor and [2]I. O. Akinyemi

[1]Department of Computer Science,
Federal College of Education, Abeokuta, Nigeria

[2]Department of Computer Science and Mathematics,
Mountain Top University, Ibafo, Nigeria

[1]sagholor@fce-abeokuta.edu.ng; alternate email: sunday.agholor@gmail.com

[2]ioakinyemi@mtu.edu.ng; alternate email: dapkin2002@yahoo.co.uk

ABSTRACT

Passwords have continued to play dominant role in online authentication systems. Consequently, it has become a great target for hackers. To mitigate these attacks, various websites have device means of educating their users on how to create strong passwords. One common form of educating users is through the existing feedback mechanism in which the user's password strength is computed and the result of the computation is displayed instantaneously as weak/good/strong. However, this form of education has been widely used for decades despite some of its drawbacks. In this work, a social class pressure system was proposed as an alternative to correct the identified flaws. The system takes the users' passwords, computes the strength and compares it with other users' passwords and reports, for example, "your password is 66% weaker than other users' passwords". With the pressure from the user's social class peers, the user will be motivated to change his password to at least a level where he/she can beat the majority of other users' passwords' strength. The system was implemented using PHP. A total of one thousand one hundred and one participants were used to test the system and existing systems for comparative analysis. The result showed that the proposed system is a better method of helping users generate strong passwords.

KEYWORDS

Better Passwords, Entropy, Existing Feedback Mechanism, Proposed Feedback Mechanism, Social Class Pressure

1 INTRODUCTION

Internet-based systems such as online banking and online commerce continue to rely heavily on passwords for access control system despite calls for its replacement by researchers [1]. Thus, passwords become the first line of defense against attacks on these systems [2]. Why are passwords widely used despite a litany of proposed replacements? The answer to this question according to [3], is because, password, as an authentication scheme is easy to learn how to use it; can easily be changed if forgotten or compromised; does not require any special hardware for implementation; and provides adequate security although there are some concerns about weak passwords which can lead to weak security. According to [4, 5], the weakness is not within the password authentication itself, but the choice of the passwords by the end-users. Furthermore, the finding of [6] revealed that the quest to replace passwords by other authentication schemes is far and difficult to achieve. Their research work led to key insights about the difficulty of replacing passwords. This finding became a motivator for usable security researchers to come up with novel approach to improve on the security of the incumbent password authentication scheme, hence the need to develop systems that will motivate end-users towards generating very strong passwords.

Research results have shown that educated users create better passwords than users that receive no guidance/education on how a good password should be created [7, 8, 9]. One common form of educating end-users is through the feedback mechanism in which the password strength meter is used to compute the strength of the end-user’s chosen password and the feedback given instantaneously.

A second approach to educating end-users is the password creation policy. According to [1], the most prevalent password creation policy is rule-based method. It functions by giving the end-users rules to be adhered to during password creation in order to create strong passwords. For example, the end-users are given the rules such as minimum password length of eight characters and must contain an upper case character and at least one special symbol character, etc.

In this work, we proposed a third approach called the Peer Pressure (Social Class Pressure) Method. In this method, the strength of the end-user’s chosen password at the point of account creation is compared with the strength of the passwords of his social class peers already in the system and the result of the comparison becomes the feedback. For example, the feedback might be “your chosen password is 66% weaker than the passwords of other users”. The detailed description of this approach is discussed at the methodology section.

The remainder of this paper is organized into four sections namely: related work, methodology, evaluation and results and finally recommendations and conclusion.

2 RELATED WORK

Several works have been done towards assisting end-users in creating very strong passwords for their numerous online accounts. Prominent among them is the feedback mechanism which relies mostly on password composition policies and password strength assessment meters. Many websites relied on existing password strength assessment meters in assisting end-users towards creating very strong passwords. This is often referred to as proactive password checker. According to [10], existing systems that check password proactively are generally based on rule sets or formulas that discourage users from using weak passwords. It has been shown by many authors that this rule-based approach in computing the password strength is not very effective [11, 12]. They therefore argued for a better formula that will drive the feedback mechanism. However, results from [7], [8] and [9] showed that the feedback mechanism helps users in creating better passwords than when there is no feedback at all.

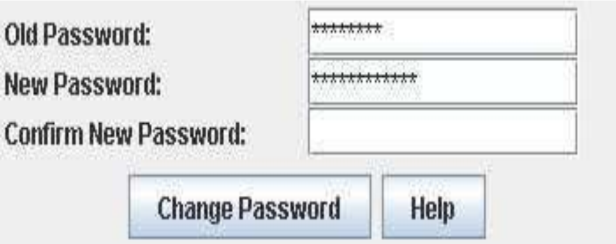
Another form of education different from the feedback mechanism was introduced by [7]. It is called Mnemonic Phrase-based Password creation method. End-users were educated to use mnemonic phrase and condensed it into a password. The advantage of this method according to [7] is that it provides equal protection with those of machine-generated random passwords but easier to remember when compared with machine-generated passwords. However, [13] cracked these mnemonic phrase-based passwords easily using mnemonic dictionary attacks. Thus, with the advent of mnemonic dictionary, there is need to research into other methods of educating the users.

In another study, [1] developed Analyzer and Modifier for Passwords using probabilistic techniques. The system first analyzes whether a user proposed password is weak or strong by estimating the probability of the password being cracked. It then modifies the password slightly if it is weak to create a strengthened password. The developed system does not allow users to modify the password by themselves. Thus, the approach is not different from the system assigned/generated password with the attendant usability problem.

In a related study, [14] developed a lightweight password creation mechanism that uses Persuasive Technology to influence users to create stronger passwords. Again, as in the case of [1], it a machine generated password approach which has more usability problem than those created by the users themselves.

Since the focus of this paper is on the effect of the feedback mechanism on the passwords created by end-users, an extensive review of the works of [15] on feedback mechanism is hereby carried out.

According to [15], the standard password selection mechanism was developed to enable users change their passwords/create new passwords. Its interface is shown in figure 1.



Old Password: *********

New Password: *************

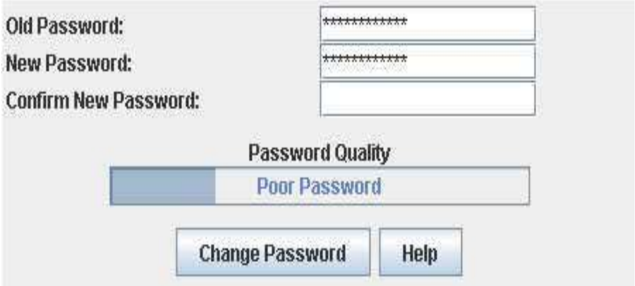
Confirm New Password:

Figure 1. A typical password selection mechanism
Source: From [15]

From figure 1, the limitations of the standard password selection mechanism are as follows:

(i) It does not assist users in creating strong passwords as it offers no security context at all.
(ii) It does not offer informative feedback to the end-users [16].
(iii) Arising from (ii), the user keep trying passwords until he or she finds the one that works but has no sense of progress from one attempt to the next [15].

To address the shortcomings of the standard Password Selection Mechanism, the current Password Selection Mechanism shown in figure 2 was developed.



Old Password: ************

New Password: ************

Confirm New Password:

Password Quality

Poor Password

Figure 2. Current password selection mechanism
Source: From [15]

As shown in figure 2, it operates by showing a progress bar that dynamically reflects the quality of the password, with a textual indicator that is updated at set thresholds informing the end-user the quality of the password chosen through a feedback mechanism [15]. End-users are encouraged to create strong passwords as a result of the feedback they receive that their chosen passwords are weak [9] and [15].

However, the drawback of this existing feedback mechanism is its non-uniformity in rating a password from one website to another. For example, an end-user's password can receive a feedback as "very strong" on a website, while the same password can receive a feedback of "weak" from another website. This type of inconsistency can bring confusion to the end-users with far reaching negative consequences.

Another commonly found drawback is that end-users, in most cases slightly modify their passwords by appending a numeric character at the end of the chosen password [17]. This, in most cases, increases the password rating from weak to strong on many websites, whereas in the actual sense such a password is vulnerable. This paper, therefore, addresses these research gaps.

3 METHODOLOGY

3.1 The Proposed Method

In this work, we proposed a method called Social Class Pressure System. It functions by influencing the user towards creating a strong password through a feedback mechanism that informs the user the strength of his password in relation to the password strength of his peers in the social class. Through this, the system adopts pressure and persuasion in influencing the user towards creating a strong password. The simplified architecture of the proposed system is shown in figure 3.

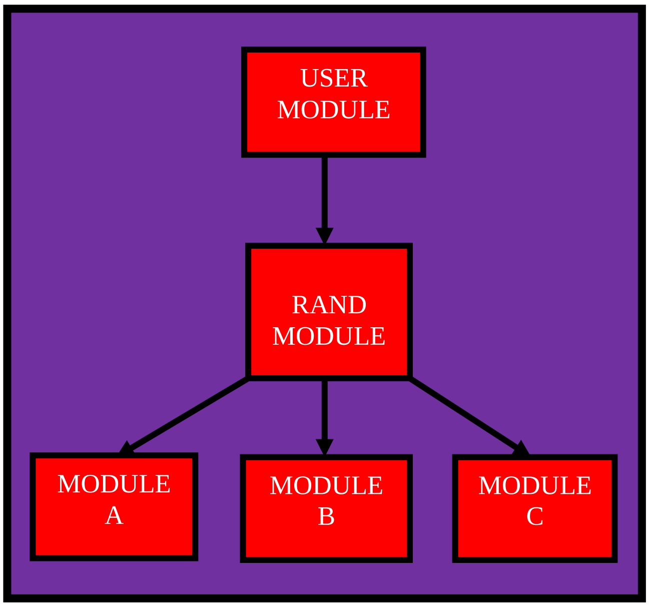


Figure 3: The Simplified Architecture of the Proposed System

The proposed system consists of five modules, namely User Module, Rand Module, Module A, Module B and Module C. The individual modules are further explained below.

3.1.1 The User Module

This module takes as an input the user password, validates it with the server and if valid, computes the entropy of the password and finally takes the user to Rand Module.

3.1.2 The Rand Module

This module uses random sampling technique in assigning users to either of Module A, Module B or Module C, where further action is required. In fact, this module is purely for random distribution of users. For example, if it assigns a user to Module A, then the dialog box for Module A will pop up to that particular user.

3.1.3 The Module A

In Module A, there is no proactive password checking mechanism. This was used as the control experiment. This module will enable us compare the strength of the changed passwords, in this case, the new passwords with the old passwords. The result from this module will enable us draw a valid conclusion on whether users can change their passwords to strong passwords without any form of education or guidance or feedback.

3.1.4 The Module B

This Module retains the existing proactive password checking mechanism using the current industry practice, that is, a horizontal bar indicating password strength in terms of very weak, weak, fair, good, strong or very strong.

3.1.5 The Module C

This module is used to test the proposed system. The module uses the social class pressure in pressuring, persuading, motivating and educating the user to creating strong password through its feedback mechanism. It takes the user's password, computes the strength and compares it with other users' passwords and gives the following feedback: "Your new password is 66% weaker than other users' passwords. Please change it immediately". With the pressure from the user's social class peers coupled with the persuasive and warning language to change the password immediately, the user will be motivated to change his password to at least a level where he/she can beat the majority of other users' passwords' strength.

3.2 The Password Strength

Password strength is a measure of the effectiveness of a password in resisting guessing and brute-force attacks. It is computed using entropy formula. In this study, we used the entropy formula of [18] to compute the password strength. The entropy formula of [18] is given by:

$$H = L*(Log(C))/(Log(2)) \qquad (1)$$

where:

H is the computed password strength;
L is the length of the password; and
C is the character set.

After computing the password strength, the system converts it to percentage. A percentage range was devised to obtain the proposed feedback mechanism. This is calculated by finding the average of each range and subtracting the resultant average from 100. The percentage range and the proposed feedback mechanism are presented in table 1.

Table 1. Password Strength and Proposed Feedback Mechanism.

Password Strength in Percentage	Proposed Feedback Mechanism
00-20	90% weaker than other users
21-30	75% weaker than other users
31-40	66% weaker than other users
41-50	55% weaker than other users
51-75	38% weaker than other users
76-99	13% weaker than other users
100-100	0% weaker than other users

3.3 Algorithm of the Model

The algorithm of the proposed System is presented below.

1. Let A, B and C be the interfaces that drive modules A, B and C respectively

```
2. Enter your old password (O_Passwd)
3. Validate O_Passwd with Server
4. If (O_Passwd is OK) then compute EntropyO
5. Interface=RAND(A, B, C)
6. If (Interface=A) then
    Enter new password (N_PasswdA)
    Compute EntropyA
    Store (O_Passwd, EntropyO)
    Store (N_PasswdA, EntropyA)
endif
     compute mean EntropyO
     compute mean EntropyA
     store (mean EntropyO, mean EntropyA)
elseif (Interface=B) then
      Enter new password (N_PasswdB)
7.    Compute EntropyB
      Convert result to percentage
      Compare with Range
      Output existing feedback mechanism
      If (N_PasswdB is changed) then goto 7
      Store (O_Passwd, EntropyO)
      Store (N_PasswdB, EntropyB)
  endif
       compute mean EntropyO
       compute mean EntropyB
       store (mean EntropyO, mean EntropyB)
else enter new password (N_PasswdC)
8.  Compute EntropyC
     Covert result to percentage
     Compare with Range
     Output new feedback mechanism
     If (N_PasswdC is changed) then goto 8
     Store (O_Passwd, EntropyO)
     Store (N_PasswdC, EntropyC)
 endif
     compute mean EntropyO
     compute mean EntropyC
     store (mean EntropyO, mean EntropyC)
END
```

4 EVALUATION AND RESULTS

4.1 Evaluation

The system was implemented using PHP and was tested using final year students of the Federal College of Education, Abeokuta, Nigeria. The students were informed that there is a new College ICT policy where each student is expected to login to the College portal, change their old passwords before printing their semester result slips. A total of one thousand one hundred and one (1,101) students were used for the evaluation test. The system uses random sampling technique in distributing the students to the three modules, where each of the modules is used to evaluate the three feedback mechanisms, namely no feedback, existing feedback mechanism and proposed feedback mechanism. Thus, each module was evaluated using three hundred and sixty-seven (367) students.

4.1.1 Module A Interface

The snapshot for Module A interface is shown in Figure 4.

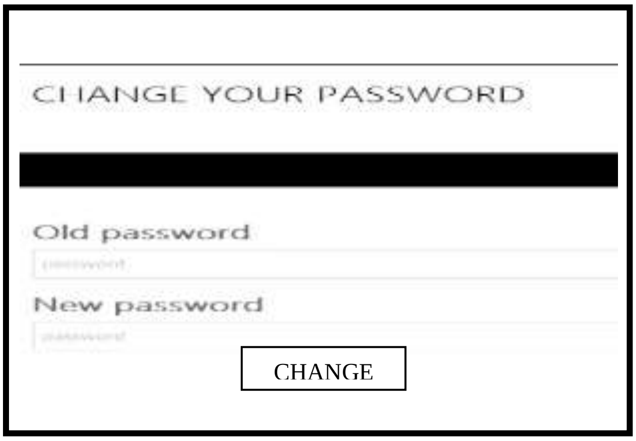
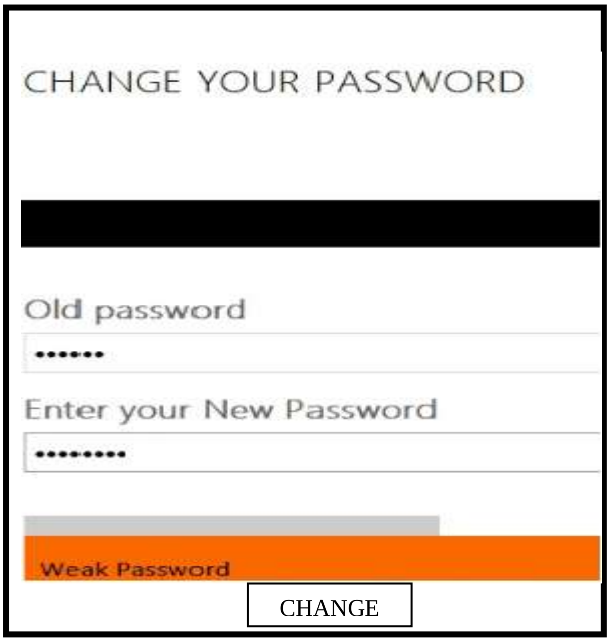


Figure 4. No Feedback

In Figure 4, one can see that there is no feedback mechanism. Here, the participants were allowed to change their passwords without any motivator driving them towards changing it to stronger passwords.

4.1.2 Module B Interface

In a related development, the snapshot for Module B interface is shown in Figure 5.



CHANGE YOUR PASSWORD

[redacted]

Old password

••••••

Enter your New Password

•••••••••

Weak Password

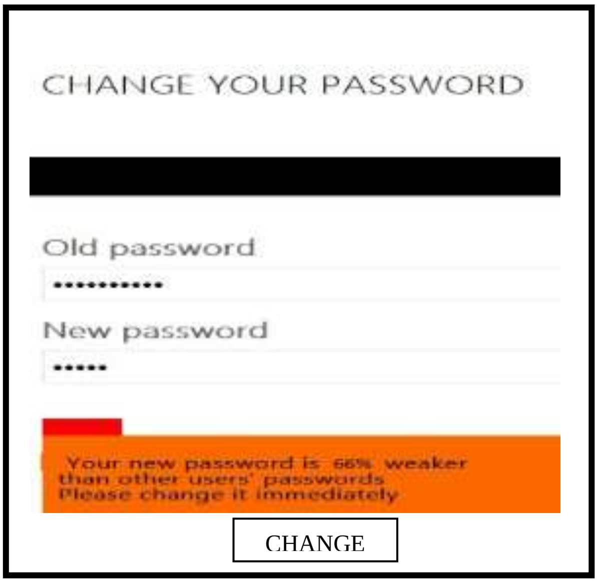
CHANGE

Figure 5. Existing Feedback Mechanism

In Figure 5, the existing feedback mechanism as currently found in majority of websites was retained. It displays the strength of the end-user’s password, thereby encouraging the end-user to change the password to a stronger one. In this case, the feedback mechanism is the motivator.

4.1.3 Module C Interface

The snapshot of Module C interface which is the interface of the proposed Social Class Pressure Method is shown in Figure 6.



CHANGE YOUR PASSWORD

[redacted]

Old password

•••••••••••

New password

•••••

Your new password is 66% weaker than other users' passwords Please change it immediately

CHANGE

Figure 6: The Proposed Feedback Mechanism

In Figure 6, one can see that the proposed feedback mechanism, which compares the strength of the end-user’s password with the passwords of the other users of the system. The aim of this type of feedback mechanism is to persuade as well as put pressure on the end-user towards changing his or her password to obtain a password strength that is at least, at par with his colleagues.

4.2 Results

The analyses of the results obtained are presented below.

4.2.1 Gender Analysis of the Sample Population

The gender analysis of the sample population is presented in table 2.

Table 2. Gender Analysis

SN	Gender	Number	Percentage
1	Male	440	39.96%
2	Female	661	60.04%
Total		1,101	100.00%

From table 2, the percentage of male is 39.96%, while that of the female is 60.04%.

4.2.2 Analysis of the new Passwords created from Module A

The mean entropy of the new passwords created using Module A was computed and compared with the mean entropy of the old passwords. The result is presented in table 3.

Table 3. Effect of no feedback mechanism on the new passwords created by Users

Password	Number of Participants	Mean Password Entropy
Old Password	367	47.43 bits
New Password	367	46.77 bits

The results from table 3 showed that both the new and the old passwords approximately have the same bit. This showed that there is no difference in password strength between the new and old passwords. Consequently, we conclude that the effect of no feedback mechanism has negative consequences on the entropy of passwords created by the end-users. This finding validated the finding of [7], [8], [9] and [15].

4.2.3 Analysis of the new passwords created from Module B

The mean entropy of the new passwords created using Module B was computed and the result compared with the mean entropy of the old passwords. The result is presented in table 4.

Table 4. Effect of existing feedback mechanism on the new passwords created by Users

Password	Number of Participants	Mean Password Entropy
Old Password	367	47.23 bits
New Password	367	56.24 bits

From table 4, the result of the study showed an increase in password strength from 47.23 bits to 56.54 bits, which is 19.08% increase in password strength. This showed that the existing feedback mechanism can help end-users create stronger passwords. It also showed that it can help end-users improve on their passwords by creating new passwords that are stronger than their old passwords. Again, the result validated the finding of [7], [8], [9] and [15].

4.2.4 Analysis of the new passwords created from Module C

The mean entropy of the new passwords created using Module C was computed and compared with that of the old passwords. The result is presented in table 5.

Table 5. Effect of the proposed feedback mechanism on the new passwords created by Users

Password	Number of Participants	Mean Password Entropy
Old Password	367	47.15 bits
New Password	367	62.35 bits

The result from table 5 showed an increase from 47.15 bits to 62.35 bits, which is 32.24% increase in password strength. This result showed that the Social Class Pressure System is a very good motivator for the end-users towards creating stronger passwords.

4.3 Discussion of Findings

The result from Module A showed a mean entropy of 46.77 bits for the new passwords, while the result from Module B showed a mean entropy of 56.24 bits for the new passwords. Furthermore, the result from Module C showed a mean entropy of 62.35 bits for the new passwords. From the results, it showed that the proposed Social Class Pressure System has the highest mean entropy.

Further analysis of the result showed that with no feedback mechanism the percentage increase in password strength is 0.00%, while the existing feedback mechanism increased the password strength of end-users by 19.08%. However, the Social Class Pressure System gave an increase in the password strength of end-users by 32.24%. Comparing the proposed system and that of the existing system, we have the mean entropy of the new password increased from 56.24 bits to 62.35 bits. This showed a percentage increase of 10.86%. Thus, we conclude that the proposed social class pressure system is a better method of helping end-users create stronger passwords.

5 RECOMMENDATIONS AND CONCLUSION

5.1 Recommendations

(1) We recommend that authentication systems that make use of existing feedback mechanism should be encouraged to adopt the proposed Social Class Pressure System and its associated feedback mechanism.

(2) We further recommend that future developers of authentication systems should adopt the Social Class Pressure System and its associated feedback mechanism.

5.2 Conclusion

The result from this study showed that Social Class Pressure is a potent method of encouraging end-users to create stronger passwords when compared with the existing feedback mechanism.

REFERENCES

[1] Houshmand, S, and Aggarwal, S.: Building Better Passwords using Probabilistic Techniques. In: Proc. of 28th Annual Computer Security Applications Conference, Orlando, Florida, USA, pp. 109-118, 2012.

[2] Gehringer, E. F.: Choosing Passwords: Security and Human Factors. In: Proc. of ISTAS, pp. 1-5, 2003.

[3] Forget, A.: A world with Many Authentical Schemes", A unpublished Ph.D. thesis submitted to the Faculty of Graduate and Postdoctoral Affairs, School of Computer Science, Carleton University, Ottawa, Ontario, Canada, pp. 1-244, 2012.

[4] Ma, W., Campbell, I., Tran, D, and Kleeman, D.: A Conceptual Framework for Assessing Password Quality. In: International Journal of Computer Science and Networking Security, vol. 7, no. 1, pp. 179-185, 2007.

[5] Gaw, S, and Felten, E. W.: Password Management Strategies for Online Accounts. In: Proc. of the 4th SOUPS. Pittsburgh, PA, USA, pp. 1-12, 2006.

[6] Bonneau, J., Herley, C., Van'Oorschot, P. C, and Stajano, F.: The quest to replace passwords: a framework for comparative evaluation of web authentication schemes. In: IEEE Security and Privacy, vol. 10, no. 1, pp. 37-48, 2012.

[7] Yan, J. J., Blackwell, A., Anderson, R, and Grant, A.: Password Memorability and Security: Some Emperical Results. In: Proc. of IEEE Security & Privacy, 2004, retrieved on 20/10/2017 from www.ieeexplore.iee.org/

[8] Sodiya, A. S, and Agholor, S.: Users Password Selection and Management Methods: Implications for Nigeria's Cashless Society. In: Proc. of 24th National Conference of the Nigeria Computer Society, Uyo, Nigeria, vol. 23, pp. 39-47, 2012.

[9] Agholor, S and Sodiya, A. S.: An Assessment of Feedback Mechanism of some Selected Websites towards improved End-Users' Password. In: Proc. of 11th International Conference of the Nigeria Computer Society, Iloko-Ijesa, pp. 44-49, 2013.

[10] Schechter, S., Herley, C, and Mitzenmacher, M.: Popularity is everything: A new approach to protecting passwords from statistical-guessing attacks. In: Proc. of 5th USENIX conference on Hot Topics in Security, Berkeley, Ca, USA, pp. 1-8, 2010.

[11] Weir, M., Aggarwal, S., Collins, M, and Stern, H.: Testing metrics for password creation policies by attacking large sets of revealed passwords. In: Proc. of 17th ACM Conference on Computer and Communications Security, pp. 163-175, 2010.

[12] Vereul, E. R.: Selecting secure passwords. In: M. Abe (Ed): CT-RSA 2007, LNCS 4377, pp. 49-66, 2007.

[13] Kuo, C., Romanosky, S, and Cranor, L. F.: Human Selection of Mnemonic Phrase-based Passwords. In: Proc. of SOUPS, New York, NY, USA, pp. 67-78, 2006.

[14] Forget, A., Chiasson, S., van Oorschot, P. C, and Biddle, R.: Persuasion for Stronger Password: Motivation and Pilot Study.In: Springer, pp. 140-150, 2008.

[15] Conlan, R. M and Tarasewich, P.: Improving Interface Designs to Help Users Choose better Passwords. In: Proc. of ACM Conference on Human-Computer Interaction, Montreal, Canada, pp. 652-657, 2006.

[16] Schneiderman, B.: Designing the User Interface: Strategies for Effective Human-Computer Interaction. 4th Ed. Addison-Wesley, 2004.

[17] Sodiya, A. S. and Agholor, S.: Users' Password Selection and Management Methods: Implications for Nigeria's Cashless Society. In: Proc. of the 24th National Conference on Towards a Cashless Nigeria: Tools and Strategies. NCS, Uyo, Nigeria, vol. 23, pp. 39-47, 2012.

[18] Shannon, C. E.: Prediction and Entropy of Printed English. In: Bell Systems Technical Journal, vol. 30, pp. 50-64, 1951.