A Preferential Analysis of Existing Password Managers from End-Users' View Point

[1]S. Agholor, [2]A. S. Sodiya, [2]A. T. Akinwale, [3]O. J. Adeniran and [2]D. O. Aborisade

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

[2]Department of Computer Science,
[3]Department of Mathematics,
Federal University of Agriculture, Abeokuta, Nigeria

[1]sunday.agholor@gmail.com

[2]sinaronke@yahoo.co.uk, [2]aatakinwale@yahoo.com, [2]daaborisade@funaab.edu.ng
[3]ekenedilichineke@yahoo.com

ABSTRACT

Existing Password Managers which are generally classified into Desktop, Online and Mobile are used for enhancing security and handling memorability of passwords by different categories of users. However, several works toward improving on the three types of Password Managers did not take into consideration the end-users' preference or choice of usage. In this work, an empirical study was conducted to determine which of the three types of Password Managers do end-users' prefer most using the following three attributes-most preferred, most convenient and most trusted. The questionnaire was first pre-tested and its reliability computed. With a reliability correlation coefficient of 0.91, the questionnaire was then administered to capture the end-users' preference and interest among the three types of Password Managers from the four thousand eight hundred and fifty (4850) participants. The results showed that 67.67% of the total participants preferred to use the Mobile Password Manager. This is followed by Online Password Manager with 16.33%, while Desktop Password Manager with 16.00% is the least preferred choice of Password Manager. From the results, the paper recommends that researchers should re-direct their efforts toward improving the Mobile Password Manager.

KEYWORDS

Desktop, End-Users, Mobile, Online, Password Manager

1 INTRODUCTION

A password is a character or sequence of characters used to determine that a device user requesting access to a system is really that particular user. Typically, users of a multiuser or securely single-user system usually have a unique name called a User-ID that can be generally known. In order to verify that someone entering that User-ID really is that person, a second identification, the password, known only to that person and to the system itself is entered by the user before access is granted. While passwords can be fairly secure, the weakness is how users choose and manage them [1, 2]. For instance, by using:

(i) Simple Passwords: These are passwords that are short in length, passwords that use words found in the dictionary, passwords created without using different character sets, passwords that are easily guessable or passwords that attackers can easily locate because they are placed on sticky notes pasted on the monitors, in a notepad or in a document stored in a computer or mobile device storage in clear text with the filename sometimes labeled as password, among other negative practices.

(ii) The same Password: This involves using the same password for multiple sites (password re-use) and never changing the password. A compromised of the password will jeopardize all accounts where the passwords have been used.

(iii) Shared Passwords: This involves a situation where users tell others, such as family members, relatives or friends their passwords, sending their password information to their friends or relatives in an unencrypted form through email for keep. This makes the password very vulnerable to the attackers.

Despite the widely circulated accounts' safety rules such as: (i) Never give your PIN, password or token digits to anyone; (ii) Do not write them down or store them on your phone or computer in an unencrypted form; (iii) Your passwords are confidential information and should never be shared with anyone; given by the banks, e-commerce, financial institutions and information security experts, some users still choose and manage their passwords using all or some of the faulty ways earlier highlighted. The reasons for these users' actions are further explained below.

The requirement of creating usernames and passwords to serve as first line of defence against unauthorized access in Web-based services such as online banking, stock trading and e-commerce application is on the increase [3] as most online services providers require users to create a username and password before using their services [3]. This has led to a phenomenal increase in the number of passwords users are expected to memorize, which to a very large extent has overstretched their cognitive abilities [4]. Consequently, users often choose easy to remember passwords which have the potential of being easy to guess by attackers.

It has been observed that as the number of the password increases, users find it more difficult to recollect the appropriate password for a particular account [5], resulting in a phenomenon called password interference. Unfortunately, the system administrator continues to impose very strict password policy requirements for the end-users [6]. These strict password policy requirements made it difficult for end-users to choose randomly generated passwords which offer high security to their account. Hence, they settle for weak passwords which offer low security. For example, as a result of human memory limitation, users often tend to choose short and low-entropy password that is easy to remember but has a possibility of being too easy to guess [7], or write down their passwords [8, 9] or use the same password at multiple websites [9, 10].

The above description is the bane of password problems: security and memorability. Unfortunately, as human, any attempt to increase one leads to a decrease in the other. But with the aid of a Password Manager, both security and memorability can be enhanced without decreasing either.

The main contribution of this study is to provide a basis for future research direction towards improving on the existing Password Managers based on end-users' choice of preference.

To the best of our knowledge, there are no empirical studies that have examined end-users' preference and interest among the three types of Password Managers. This is the source of our motivation.

The rest of this paper is organized as follows: In Section 2, the Literature Review was discussed, while Research Methodology was discussed in Section 3. In Section 4, the collected data were analyzed and the results discussed, while Conclusion and Recommendation were discussed in Section 5.

2 LITERATURE REVIEW

The single most important step that can be taken to improve password security thereby addressing the weakness of a password earlier highlighted, is by increasing its entropy [11], hence [12] recommended a password that is randomly generated from all character sets with an appreciable length. This, no doubt will help address the findings of [13] and [14]. However, increasing the password entropy helps in increasing the password strength but not without a trade-off, the memorability crisis.

In attempt to solve the twin problems of passwords, that is, security and memorability, highlighted earlier, [7] suggested the use of mnemonics in constructing passwords. The result from this study showed that mnemonic-based passwords offered equal protection as those of randomly-constructed passwords. Furthermore, the finding showed that mnemonic-based passwords are easier to remember than randomly-constructed passwords. However, [15] found that [7] used basic dictionary attacks in their experiment, hence they constructed mnemonic-based dictionary which was used to attack the mnemonic-based passwords. Their findings which contradicted that of [7] revealed that mnemonic-based passwords could be cracked with the use of mnemonic dictionary attack. Thus, to prevent their accounts against hacking, end-users have no option other than to use highly random passwords of appreciable length [12]. Again, this comes with a trade-off, that is, memorability.

To avert memorability problem usually associated with the use of different complex passwords, many end-users resort to self help by using the same password for different online accounts. This is often referred to as password re-use. In a survey conducted by [16], 81.00% of the subjects admitted re-using the same password on many websites, while 68.00% admitted selecting related but not necessarily identical passwords across sites. In a related development, [13] findings showed that 18.75% re-use passwords, while 25.00% admitted using closely related password to access each account. Unfortunately, this action of re-using the same password for many online accounts increases security risk to the end-user whenever the password is breached [17]. Similarly, the investigation carried out by [18] on password usage in companies and that of [19] on the effects of password policies on users' practices, revealed alarming negative password practices caused by memorability problem.

Notwithstanding the wide-held sentiments from the security and usability communities that password should be replaced by other authentication schemes, it is likely to remain the most dominant authentication scheme [13, 20, 21, 22, 23, 24, 25, 26]. The reason for this is as a result of its incumbency, familiarity, and low cost in terms of its implementation, as well as inability of information security experts to reach a consensus on what exactly the alternative should provide [27]. According to [28], the 2005 RSA Conference panel communiqué stated that password has come to stay and will be with us forever. They, therefore, called on information security researchers to come up with measures that will make the use of password simpler and effective. Supporting this assertion is [1] who stated that password authentication is still and will continue to be the working horse of information security. These claims are still valid today as online accounts that require password is on the increase for a particular user. This is why research effort should be channeled towards improving its security and memorability. One way of doing this is through the use of Password Managers.

Password Managers were developed to relieve the end-users the burden of memorability [20]. It only requires the user to create and remember a single Master Password, ideally, a very strong password which grants the user access to their entire password database. According to [29], remembering a single Master Password is much more feasible for users, who still get the security benefits of using a different password for each online service.

Password Managers can also be used as a defence against phishing and pharming attacks. Unlike human beings, a Password Manager can also incorporate an automated login script that first compares the current site's URL to the stored site's URL. If the two did not match, then the Password Manager does not automatically fill in the login fields. This is intended as a safeguard against visual imitations and look-alike websites. With this built-in advantage, the use of a Password Manager is beneficial even if the user only has a few passwords to remember. In addition, Password Managers can protect against keyloggers or keystroke logging malware. When using a multi-factor authentication scheme, a Password Manager can automatically fill-in the field for login. The user does not have to type any user names or passwords for the keylogger to pick up. However, Password Manager cannot protect against man-in-the-browser attacks, where malware on the user's device performs operations hidden from the user when the user is logged in.

2.1 Overview of existing Password Managers

We present below a brief overview of the Password Managers which according to [30] are generally classified into Desktop, Online and Mobile Password Managers.

2.1.1 Desktop Password Manager

They are used to store multiple passwords on local computers or the user's desktop, that is, on the terminal used for authentication which in turn is protected by a Master Password and can be retrieved when users revisit the websites through that computer. It is often called Offline Password Manager. Users are only required to memorize the Master Password. This Password Manager has the advantages associated with using Password Managers highlighted earlier. However, it has the following disadvantages: It is not portable, it is vulnerable to offline and online attacks. Examples are RoboForm, Mozilla Firefox, Apple MacOS Keychain, Microsoft Internet Explorer etc.

2.1.2 Online Password Manager

Online Password Manager stores the passwords on remote third-party server(s). It is also called Web-based or Cloud-based Password Manager. The passwords are typically protected using a Master Password and at the time of recalling a specific password, the user simply types in his Master Password. The user of this Password Manager enjoys the advantages of its portability, in addition to the general advantages of using Password Manager earlier enumerated. However, the disadvatages include: Vulnerable to offline and online attacks, vulnerable to network failure, and requires the user to trust the third party server in which the passwords are stored as a disgruntle staff of a third party provider can manipulate the data to his advantage. In other words, the user has no control in the management of his passwords. Examples are LastPass, MozillaWeave Sync, etc.

2.1.3 Mobile Password Manager

A Mobile Password Manager stores passwords on end-users' portable devices such as phones and USB devices. Again, the passwords are typically protected using a Master Password and at the time of recalling a specific password, the user simply types in his Master Password. The user of this Password Manager enjoys all the advantages of a Password Manager earlier highlighted, in addition to the advantages of controlling and managing his passwords locally by himself on his portable device. However, the use of this Password Manager has some disadvantages such as vulnerable to offline and online attacks, vulnerability to lost of mobile devices, in addition to the mobile device becoming a target for thieves. Examples are KeePassmobile, OpenIntents Safe, Roboform2Go etc.

3 RESEARCH METHODOLOGY

The study was conducted to enable us determine the end-users' preferences and interests among the three types of Password Managers. We describe the overview of the procedure used in carrying out this study.

The first stage was the establishment of the population of the study, which consists of all the twenty four (24) tertiary institutions in Ogun State of Nigeria.

In the second stage, the questionnaire was identified as the instrument to be used for data collection. The questionnaire after its construction was first administered to a selected sample from the population and later re-administered to the same sample population. The reliability of the questionnaire was evaluated by computing the correlation coefficient of the results obtained. With a correlation coefficient of 0.91, we conclude that the research instrument is reliable enough to be used for the field work.

The third stage was the selection and training of the sample population on how to use Password Managers. For the sample population, eighteen (18) schools were selected out of the twenty four (24) tertiary institutions using stratified random sampling. Thus, the sample size for the study when compared to the population is 75%. Next was the training of the sample population on how to use a Password Manager. At the first phase, they were trained on how to use Desktop Password Manager and were allowed to use it for two (2) months. In the second phase, they were trained on how to use Online Password Manager. Again, they were allowed to use it for two (2) months. At the third phase, they were trained on how to use Mobile Password Manager and were allowed to use it for two (2) months.

It should be reported that during the training, we observed that majority of the sample population were already using one form of Password Manager or the other. This made our training easy and simple for the sample population.

The final stage was the random administration of four thousand eight hundred and fifty (4850) questionnaires to the trained sample population which comprised of students, lecturers (faculty staff) and non-academic staff. The number of questionnaires collected back for analyses was four thousand five hundred (4500). This showed that 92.78% of the total questionnaires administered were returned for analyses. In other words, the return rate is high enough to enable us draw meaningful inference from the analyses.

4 ANALYSES, RESULTS AND FINDINGS

4.1 Demographic Characteristics of the Participants

The study analyzed the demographic variables which comprise of age, sex and educational status of the participants. The result is presented in table 1.

Table 1. Demographic Characteristics of the Participants

Parameter	**Frequency**	**Percentage**
AGE (YEARS)		
18-30	1423	31.62%
31-40	1173	26.07%
41-50	1045	23.22%
51-60	859	19.09%
Total	**4500**	**100.00%**
SEX		
Male	2340	52.00%
Female	2160	48.00%
Total	**4500**	**100.00%**
LEVEL OF EDUCATION		
Students (O/L Certificates)	2259	50.20%
ND/NCE/HND/First Degree	1080	24.00%
Masters	981	21.80%
Ph.D.	180	4.00%
Total	**4500**	**100.00%**

From table 1, the minimum age of the participants is 18 years, while the maximum age is 60 years. This shows that the sample population is age-centric. The inference that could be drawn from this analysis showed that the participants represent an active age bracket that uses Password Managers.

Furthermore, table 1 shows that a little above half of the participants (52.00%) are male, while 48.00% of the participants are female. Statistically, we conclude that the study used a sample population that is gender-centric.

In the same vein, the distribution of the participants according to their educational status shows that 50.20% are students of the tertiary institutions, which implies that 50.20% of the respondents have Ordinary Level (O/L) Certificates, while 24.00% are in the category of those having qualification that are higher than O/L but not above first degree, 21.80% are holders of Masters degree, while 4.00% are Ph.D. holders. Thus, the educational level of the sample population is high enough and it is a good representation of those that can fill the questionnaire without assistant or guidance.

4.2 Participants' use of Passwords and Password Manager Experience

We captured the number of passwords each participant has been managing as well as the years of experience of using all or any of the three different types of Password Managers before the training.

(a) Number of Passwords in use by the Participants

Participants were asked to indicate the number of different passwords they use to authenticate to their various online accounts. The result is as presented in table 2.

Table 2. Number of Passwords own by the participants

No. of Passwords	No. of Participants	Percentage
1-5	150	3.33%
6-10	1800	40.00%
11-15	900	20.00%
16-20	750	16.67%
21-25	540	12.00%
>25	360	8.00%
Total	4500	100.00%

From table 2, one can see that 12.00% of the participants have between 21 and 25 passwords, while 40.00% of the participants have between 6 and 10 passwords. From this analysis, it showed that the participants need Password Manager to manage their numerous online accounts. This data is further explained using figure 1.

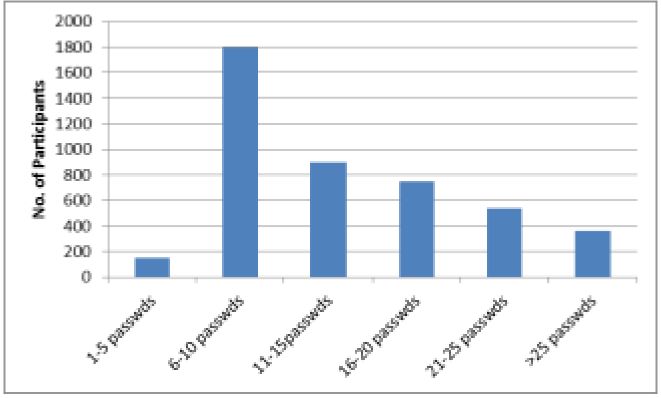

Figure 1. Bar Graph showing the number of passwords own by the Participants

(b) Participants' Experience in the use of Password Managers

In this section, we captured the participants' experience in the use of Password Managers. The result is presented in table 3.

Table 3. Participants' Experience in the use of Password Managers

Years of Experience	No. of Participants	Percentage
Less than 1 year	225	5.00%
1-2 years	1125	25.00%
3-4 years	2250	50.00%
Above 4 years	900	20.00%
Total	4500	100.00%

Table 3 shows the years of experience of using a Password Manager by the participants. From table 3, it shows that 50.00% of the participants have been using Password Managers for a period of 3 to 4 years, while 20.00% have been using Password Managers for more than 4 years. This shows that the participants have enough relevant experience to be used for the conduct of our study. This data can further be explained pictorially using figure 2.

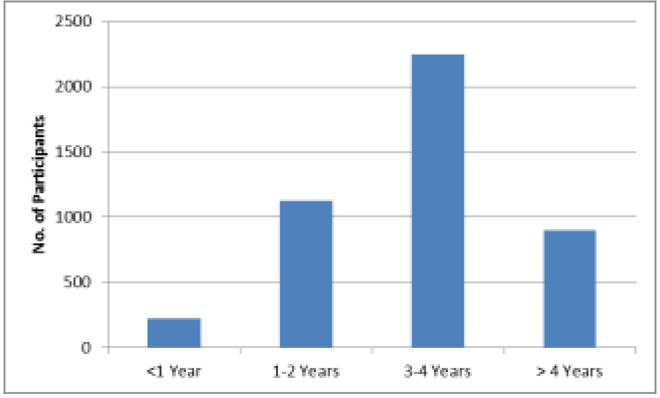

Figure 2. Bar Graph showing the Partcipants' Experience

4.3 Preferential Analyses

The preferential analyses for Most Preferred, Most Convenient and Most Trusted Password Manager (PM) are presented in tables 4, 5 and 6.

(a) Analysis of Most Preferred Password Manager

Table 4 shows the analysis of the Most Preferred Password Manager.

Table 4. Analysis of Most Preferred Password Manager

Password Manager	No. of Participants	Percentage
Desktop	900	20.00%
Online	720	16.00%
Mobile	2880	64.00%
Total	4500	100.00%

From table 4, one can see that 64.00% of the participants prefer to use Mobile Password Manager, while 20.00% of the participants prefer to use Desktop Password Manager. Trailing behind is the Online Password Manager with 16.00% of the participants taking it as their preferred choice of Password Manager. From the result, it shows that most end-users prefer to use the Mobile Password Manager. This is further explained pictorially using figure 3.

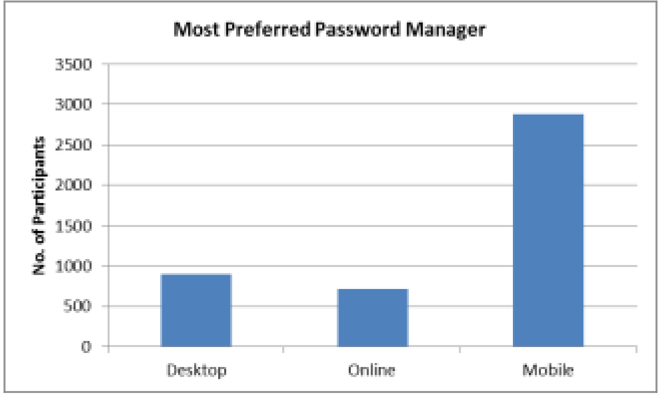

Figure 3. Bar Graph showing the Most Preferred Password Manager

(b) Analysis of the Most Convenient Password Manager

Table 5 shows the analysis of the Most Convenient Password Manager.

Table 5. Analysis of Most Convenient Password Manager

Password Manager	No. of Participants	Percentage
Desktop	450	10.00%
Online	1035	23.00%
Mobile	3015	67.00%
Total	4500	100.00%

In table 5, it is seen that 67.00% of the participants affirmed that Mobile Password Manager is the most convenient for them to use, while 23.00% opted for Online Password Manager as the most convenient for them to use and 10.00% said that Desktop Password Manager is the most convenient for them to use. From this result, we conclude that Mobile Password Manager is the most convenient for the end-users to use. Pictorially, this is further explained using figure 4.

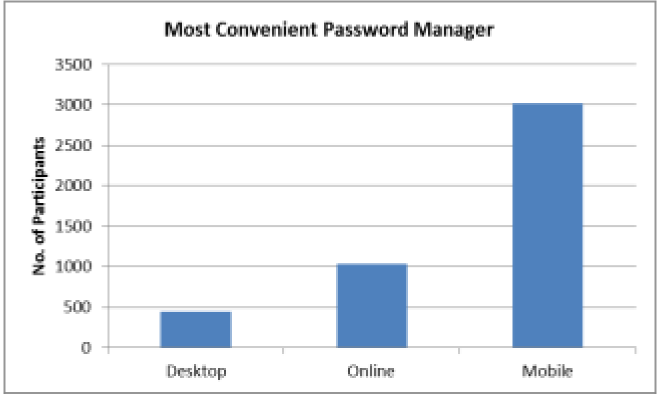

Figure 4. Bar Graph showing the Most Convenient Password Manager

(c) Analysis of the Most Trusted Password Manager

Table 6 shows the analysis of the Most Trusted Password Manager.

Table 6. Analysis of Most Trusted Password Manager

Password Manager	No. of Participants	Percentage
Desktop	810	18.00%
Online	450	10.00%
Mobile	3240	72.00%
Total	4500	100.00%

The result in table 6 shows that a very high percentage, that is, 72.00% of the participants said that the Mobile Password Manager is their most trusted, with 18.00% accepting Desktop Password Manager as their most trusted and only 10.00% agreed that Online Password Manager is their most trusted. Using this result, we conclude that Mobile Password Manager is the most trusted Password Manager that end-users will be willing to use. This is further explained pictorially using figure 5.

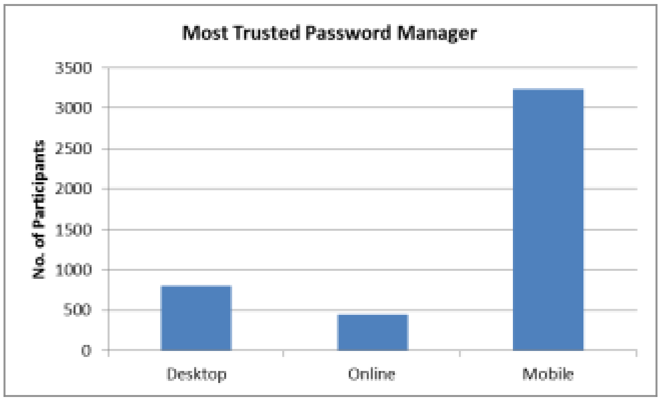

Figure 5. Bar Graph showing the Most Trusted Password Manager

(d) Overall Analysis of End-users' Choice among the three categories of Password Managers

The overall analysis of the end-users' preference among the three categories of the Password Managers is presented in table 7. This utilizes the aggregate of the three attributes, that is, the most preferred, most convenient and most trusted.

Table 7. Overall Analysis of the three categories of Password Managers

Password Manager	Most Preferred		Most Convenient		Most Trusted		Overall % Average
	No.	%	No.	%	No.	%	
Desktop	900	20	450	10	810	18	16.00
Online	720	16	1035	23	450	10	16.33
Mobile	2880	64	3015	67	3240	72	67.67
TOTAL	4500	100	4500	100	4500	100	100

Table 7 shows the percentage of end-users who preferred a particular Password Manager. From the result, the order of preference turned out to be Mobile (67.67%), followed by Online (16.33%) with Desktop (16.00%) being the least preferred choice of Password Manager. From the above findings, it showed that the end-users were not comfortable giving control of their password management to a third party. Hence, they preferred to manage their passwords themselves on their own mobile phones. It is evident from the findings that the Mobile Password Manager gives them high degree of confidence when using it as their Password Management Scheme. Pictorially, the percentage overall analysis can be explained using figure 6.

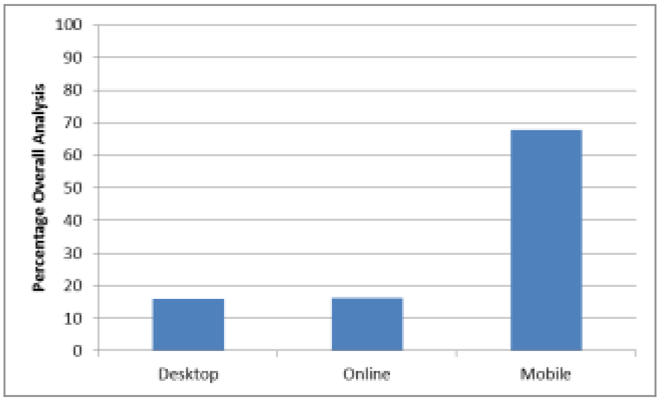

Figure 6. Bar Graph showing the overall percentage Analysis

5 CONCLUSION AND RECOMMENDATION

The results of this study showed that the Mobile Password Manager is a more promising password management scheme than the Online and Desktop Password Managers.

From the findings, we recommend that research effort should be directed towards improving the architecture of the Mobile Password Manager. This will enhance the ergonomics of the Password Manager.

Secondly, we recommend that more research work towards protecting the passwords stored in the Mobile Password Manager especially against offline and online attacks should be carried out.

REFERENCES

1. Ma, W., Campbell, J., Tran, D., Kleeman, D.: A Conceptual Framework for Assessing Password Quality. In: International Journal of Computer Science and Network Security, vol. 7, no. 1, pp. 179-185 (2007).

2. Gaw, S., Felten, E. W.: Password Management Strategies for Online Accounts. In: Proc. of the 2nd Symposium On Usable Privacy and Security (SOUPS), ACM, pp. 44-55 (2006).

3. Dhananjay, K., Fredrick, C. S.: iPass Framework to Create Secure and Usable Passwords. In: CSS, Chicago, USA (2009).

4. Halderman, A., Waters, B., Felten, E.: A convenient method for securely managing passwords. In: Proc. of World Wide Web Cobference, Chiba, apan, pp. 471-479 (2005).

5. Aborisade, D. O., Alowosile, O. Y., Odunlami, K. O., Odumosu, A.: A Cloud-based Password Manager for Multiple Transactions Accounts. In: Proc. of 11th International Conference of Nigeria Computer Society, Iloko-Ijesa, Nigeria, pp. 3-10 (2013).

6. Schechter, S., Herley, C., Mitzenmacher, M.: Popularity is Everything: A new approach to protecting passwords from statistical-guessing attacks. In: Proc. of the 5th USENIX Conference on Hot Topics in Security, Berkeley, USA, pp. 1-6 (2010).

7. Yan, J. J., Blackwell, A., Anderson, R., Grant, A.: Password Memorability and Security: Some Emperical Results. In: IEEE Security & Privacy, pp. 1-8 (2004). From www.ieeexplore.ieee.org/ie15/8013/29552/ 0134406. pdfAccessed on 20/08/2011.

8. Zhang, J., Luo, X., Akkaladevi, S., Ziegelmayer.: Improving Multiple-Password Recall: An Emperical Study. In: European Journal of Information Systems, vol.8, pp. 165-176 (2009).

9. Sodiya, A. S., 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).

10. Moshfeghian, S., Ryu, V. S.: Your Password is Invalid: Improving website Password Practices. In: Science Daily, pp. 1-8 (2012). From www.sciencedaily.com/release/2012/01... Accessed on 25/05/2012

11. Gayathiri, C.: Text Password Survey: Transition from First Generation to Second Generation, pp. 1-10 (2013).

12. Agholor, S., Sodiya, A. S., Akinwale, A. T., Adeniran, O. J.: A Secured Mobile-Based Password Manager. In: Proc. of IEEE 6th International Conference on Digital Information Processing and Communications, Beirut, Lebanon, pp. 103-108 (2016).

13. Soluade, O. A., Opara, U. E.: Security Breaches, Network Exploits and Vulnerabilities: A Conundrum and an Analysis. In: International Journal of Cyber-Security and Digital Forensics, vol. 3, no. 4, pp. 246-261, (2014).

14. Ale, J. H., Hussin, J. H., Jose, A. H.: Cyber Warefare Awareness in Lebanon: Exploratory Research. In: International Journal of Cyber-Security and Digital Forensics, vol. 4, no. 4, pp. 482-497, (2015).

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

16. Bojinov, H., Bursztein, E., Boyen, X., Boneh, D.: Kamouflage: Loss-Resistant Password Management, pp. 1-16 (2010). From www.cryto.stanford.edu. Accessed on 11/12/2014

17. Wessels, P. L., Steenkamp, L. P.: Assessment of current practices in creating and using passwords as a control mechanism for Information Access. In: South African ournal of Information Management, vol. 9, no. 2, pp. 1-15 (2007).

18. Inglesant, P., Sasse, M. A.: The True Cost of Usable Password Policies: Password Use in Wild. In: Proc. of ACM Conference on Human-Computer Interaction, New York, USA, pp. 383-392 (2010).

19. Shay, R., Komanduri, S., Kelly, P. G., Mazurek, M. L., Bauer, L., Christin, N., Cranor, L. F.: Encountering Stronger Password Requirements: User Attitudes and Behaviors. In: Proc. of SOUPS, Redmond, pp. 1-15 (2010). From www.cups.cs.cmu.edu/soups/2010... Accessed on 23/12/2013.

20. McCarney, D., Barrera, D., Clark, J., Chiasson, S., Van'Oorschot, P. C.: TAPAS: Design, Implementation and Usability Evaluation of a Password Manager. In: Proc. of the 28th Annual Computer Security Applications Conference, Orlando, Florida, USA, pp. 89-98 (2012).

21. Shiva, H. Y., Aggarwal, S.: Building Better Passwords using Probabilistic Techniques. In: Proc. of the 28th Annual Computer Security Applications Conference, Orlando, Florida, USA, pp. 109-118 (2012).

22. Preet, I. S., Gour, S. M. T.: Enhanced Password Based Security System based on User Behavior using Neural Networks. In: International Journal of Information Engineering and Electronic Business, vol. 2, pp. 29-35 (2012).

23. Florencio, D., Herley, C.: Where Do Security Policies Come From? In: Proc. of SOUPS, New York, USA, pp. 1-14 (2010).

24. Dell' Amico, M., Michiardi, P., Roudier, Y.: Password Strength: An Emperical Analysis. In: Proc. of INFOCOM, San Diego, pp. 983-991 (2010).

25. Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., Memon, N.: Passpoints: Design and Longitudinal Evaluation of Graphical Password System. In: International Journal of Human-Computer Studies, vol. 63, pp. 42-49 (2005).

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

27. Herley, C., Van’ Oorschot, P. C.: A research agenda acknowledging the persistence of passwords. In: IEEE Security & Privacy, vol. 10, no. 1, pp. 28-36 (2012).

28. Saita, A.: Passwords at the breaking points. In RSA 2005 Conference Panel Communiqué, pp. 1-6 (2005). From www.searchsecurity.techtarget.com/.... Accessed on 22/10/2011.

29. Gasti, P., Rasmussen, K. B.: On the Security of Password Manager Database Formats. In: Computer Security, vol. 7459, pp. 770-787 (2012).

30. Karole, A., Saxena, N., Christin, N.: A Comparative Usability Evaluation of Traditional Password Managers, pp. 1-15 (2010). From www.cis.uab.edu/saxena... Accessed on 13/09/2012.