Memorability Interference Level for Multiple Modes of Authentication.

A.O. Egwali, Ph.D.* and Prof. Emmanuel A. Onibere

Department of Computer Science, Faculty of Physical Sciences, University of Benin, PMB 1154, Benin City, Edo State, Nigeria.

E-mail: egwali.annie@yahoo.com*

Telephone: +234(0)7033247730*

ABSTRACT

Extensive password requirements overload human memory capabilities as the number of passwords and their complexity levels increase. This is evident in the use of textual password (TP) models that have been plagued with security and usability problems. Several factors like users' behavior, operational platform and system design has been attributed to these problems. But there exist no known study of password interference level for multiple mode of authentication and it relationship with users' memory capability and submission pattern.

Presented in this paper is the first objective of an on-going web study conducted to verify the password interference level for multiple modes of password authentication using TP, mnemonic passwords (MP), Shield-1 (a graphical password model), and Shield-2 (a graphical password and fingerprint biometric system). Report from our web study shows that the success rates of Shield-2 and Shield-1 passwords performed better than those of MP and TP models. It is strongly believe that memory cueing provided by images is a major reason for enhanced users' success rates and recall performance, followed by familiarity based on frequent usage as is the case with TP. Authentication models can also be significantly impacted by training, interference alleviation and frequency of usage.

(Keywords: graphical password, authentication, passwords, fingerprint biometrics, mnemonic password)

INTRODUCTION

Some organizations have devised strategies to make passwords memorable to users by introducing mnemonic passwords (MP), which have the capability to counter some of the deficiencies of textual passwords (TP). To derive MP, users are instructed to think of memorable phrases that are not less than seven words that are not guessable but easy to remember. And by representing some of these phrases with numbers, symbols, and letters (i.e., first letters), the MP is derived. Nonetheless, MP should not be regarded as the absolute solution for the TP dilemma, for they still do not remove the possibility of vulnerabilities like shoulder surfing attacks where other illegitimate users can view them being typed or social engineering attacks where a legitimate user is forced to reveal or write down their passwords on paper.

Graphical password (GP) models have also been proposed as a possible alternative to TP, motivated by the facts that human can remember pictures better than text (Moncur and Leplâtre, 2007). GP systems take three basic forms, which are: recognition based systems in which a user chooses images or icons or symbols from a large collection to be authenticated, and then the users need to recognize and identify the images, icons or symbols he or she selected during the enrolment stage; and recall-based system (which is further classified under pure recall models and cued recall models). In cued recall, users have to recall a password, but the system offers a framework of hints, context and cues that help the users reproduce their passwords or help them make the reproduction more accurate. Pure recall-based GP systems are occasionally referred to as draw metric systems (DeAngeli, et al., 2005). However, Wiedenbeck, et al., (2005) stated that the nature of the images used in a system may have a large effect on people's ability to remember their click points.

Biometrics identification of a person is based on his or her physiological or behavioral

characteristics. Generally to authenticate, a user enters an account, username, or inserts a token such as a smart card, but instead of entering a password, a simple touch with a finger or a glance at a camera is enough to authenticate the user (Fernando et al, 2005). Biometric-based models provide the same level of security to all users and the biometric signal is difficult to steal or forge. Users' inconveniences are also alleviated because they do not need to memorize long and random passwords.

In distinguishing individuals, each biometric trait has a hypothetical upper bound and fingerprint representations possess better discrimination capability (Pankanti, et al., 2002) in comparison to face biometrics (10^3) and hand geometry (10^5) that have a limited number of distinguishable patterns that result in poor quality images that fall short of the high accuracy requirements of critical applications (O'Gorman, 2003). Despite these obvious advantages, the use of biometrics raises several security, usability, and privacy concerns.

Based on the perception of several leading biometric authorities, no single biometric can satisfy all the biometric characteristics, which includes: universality, uniqueness, permanence, collectability, performance, acceptability, circumvention resistance and effective costs (Jain, et al., 1999; Scheuermann, et al., 2002). Generally, single modal biometric systems are non-universal in nature. For example, the National Institute of Standards and Technology (NIST, 2002) has reported that it is not possible to obtain a good quality fingerprint from approximately two percentage of the population and hence such people cannot be enrolled in a fingerprint biometric system. For this study a multifactor approach is employed.

Past researched studies on user authentication models have included studies on the usability and security of individual modal systems, in which TP is compared with biometric system (Ratha, et al., 2001), MP (Onibere and Egwali, 2011), tokens (Carstens, et al., 2004; Yan, et al., 2004; Zviran and Erlich, 2006) and GP models (Alireza and Angelos, 2008; Behzad, et al., 2008; Onibere and Egwali, 2011). It has also included users' performance when using multiple TP at different sites, users' password management and users' short-term memory challenges in managing single and multiple GP models (Fraser, 2006, Tari, et al., 2006).

In practice, as newer and better authentication models are developed, users will be challenged with the task of not only handling more authentication models concurrently, but models with diverse inbuilt techniques and user requirements. This definitely will generate new challenges than that from single modal systems. However there is a dearth of knowledge on the relationship between users' memory capability and multiple modes of authentication.

To address users' challenges in complying with conflicting extensive password requirements which overloads the human memory capabilities, this study is conducted on four different authenticating models: TP, MP, shield-1 (a GP model) and Shield-2 (a graphical and fingerprint biometric model) authentication models, and verify the password interference level for multiple TP, MP, Shield-1, and Shield-2.

The research study examines the relationship between users' memory capability and multiple modes of authentication by studying the performance of users authenticating with four dissimilar inbuilt authenticating password techniques and user requirements. The study also explores the interference effect among each authenticating model password techniques and users password pair. This further aid in establishing the severity of users' memorability challenges.

MATERIALS AND METHODS

A field study is conducted on four different authenticating models: TP, MP, Shield-1 (a GP model), and Shield-2 (a graphical and fingerprint biometric model) authentication models, to verify the password interference level for multiple TP, MP, Shield-1 and Shield-2.

The image set for Shield-1 and Shield-2 were taken from a wide range of backgrounds which includes religious, nature, life's philosophy, family, education, goals, food, hobbies etc., which significantly increases security. The choice of an online study instead of a laboratory study is based on the fact that the online study would provide access to a larger class of user population and would provide the enabling environment for users to authenticate under more realistic sceneries. The four authenticating models were selected because users can

securely remember about four or five dissimilar passwords (Adams and Sasse, 1999).

Within-subjects design experimentation is used to compare multiple password interference for each model usage conditions. There are three different major activities that users can perform in each model usage: (1) multiple-password training, (2) multiple-password registration (password creation) and (3) multiple-password recall (during subsequent login). These activities are classified into two sessions. Session one involves training on how to register and login with the different models and the filling of an online questionnaire. Session two involves the actual registration and login of users to access online materials.

Section One: Training Session and Questionnaire Assessment

To attract users to the webpage designed for the web study, some lecturers in Computer Departments from four different educational institutions: University of Benin in Edo state, Benson Idahosa University in Edo State, Crawford University Oye-Ekiti in Ekiti State, and Rufus Giwa Polytechnic in Ondo State were informed to direct their students to the website to access e-books, course notes, job offers, tutorial materials, etc. No direct effort was made to contact students to use the system. To remove any bias as to the order in which participants utilize the system, all four models was made available and can be utilized in parallel as desired by users.

In the training sessions, each authentication model session begin with an automated PowerPoint tutorial presentation that introduces and explain the authentication procedures needed to login into the sites using the four models. The rules for creating the different passwords were made clear to participants (Table 1).

For example, to register for Shield-1, users were instructed to first enter their full name, e-mail address and then select and enter the codes of each corresponding image of choice by making use of the keyboard instead of the mouse. A minimum of six and a maximum of ten images and their corresponding codes (graphical passwords) need to be selected. During the login stages, the participant only provides the registered email and GP.

In the case of Shield-2, users were instructed to first enter their full name, e-mail address and enter the codes of each corresponding image of choice by making use of the keyboard. The registration submission button takes the user to the fingerprint registration wizard interface, which contains instructions for participants to register a fingerprint. The software application was designed to interact with FingerAuth, an Add-on Extension for Mozilla Firefox, which captures and authenticate the fingerprints of the user using an optical fingerprint sensor device with an image resolution of 500 DPI + 0.2%, an image size (pixels) of 260 x 300, an image capture speed of 2.3 frames/second and an image transfer speed of 308 kbps.

Table 1: Rules for Creating Passwords.

Models	Password Rules
Shield-1	1) Choose images passwords from the image set. 2) Enter the numbers below the images on the boxes below each image. 3) Follow any diagonal pattern while choosing. 4) Password must not be less than six (6) image codes and greater than ten (10).
Shield-2	1) Choose images passwords from the image set. 2) Enter the numbers below the images on the boxes below each image. 3) Follow any diagonal pattern while choosing. 4) Password must not be less than six (6) image codes and greater than ten (10). 5) Register a fingerprint against your password
Mnemonic	1) Enter a MP by choosing an expression of your choice and abbreviating it. 2) Password must be greater than six (6) characters. 3) MP must contain lowercase alphabets, uppercase alphabets and numbers.
Textual	1) Enter passwords which are either plainly lower case letter or uppercase letter or numbers or symbols or the combination of the four 2) Passwords must not be less than six (6) characters. 3) Passwords must contain lowercase alphabets, uppercase alphabets and numbers.

The device software driver extracts the minutiae points from the fingerprint image data, and converts the data into a unique mathematical template, comparable to a 60 digit password. Participants' fingers of choice must be place in the fingerprint sensor device for the system to scan the finger four times in order for the registration to be established. As each finger is placed on the sensor, the system automatically reads the fingerprint four times until a message indicates that the scan is successful and that the participant registration has been completed. During the login stages, the participant provides the registered email and the initially registered finger. Very few participants who were chosen at random were made to use Shield-2, these include novice computer users and experienced computer users and they are permitted to login from any machine (home, school, etc.).

To register with the MP model, participants were instructed to first enter their full name, e-mail address, full expression and the MP equivalent of the expression. As users entered their MP, it is echoed only as asterisks. However, the MP must be greater than 6 characters and must contain lowercase alphabets, uppercase alphabets and numbers. During the login session, the participants only had to provide the registered emails and MP. To register with the TP model, participants were instructed to first enter their full name, e-mail address and a password which must be greater than 6 characters and must contain lowercase alphabets, uppercase alphabets and numbers. As users entered their password, it is also echoed only as asterisks. Subsequently, to login, the participants were only to provide the registered emails and passwords.

The tutorial concludes with a directive for participants to engage in a training session. Participants are allowed to experiment with training modules and register their authentication credentials and login as many times as they wanted with the system responding with a message in each case if the password is accepted or not accepted. At the end of the training (learning) session (i.e., immediately after clicking the submission button), participants were made to fill an online questionnaire that contains participants demographic information and AC choices and other authenticating information required. The filling of the questionnaire took about 15 minutes, this time frame acted as a distractor between the learning phase and the first retention trial. The 15 minutes distraction was presented to remove the passwords from users' visual working memory, since psychology literature suggests that 15-30 seconds is ample time for this to occur (Goldstein, 2006).

Section Two: Actual Authentication and Login Sessions

After the period of memory tasks, activating the submission button that submit the questionnaire form to the database, upload the authentication interface for participants to actually register and log into the system. In the actual registration and login sessions which comes after the training (learning) phase, irrespective of the model used, participants had the opportunity to reselect any authenticating model of their choice irrespective of what they had used for the training phase to login to view online information. Instructions on the screen acted as guides to enable participants create valid passwords. If a participant was unable to remember his/her password, another choice had to be made or the training session can be visited again.

Users Accounts

Users either registered or logged into the site using any of the four models. At this stage, the research site was able to capture a total of 1586 site accounts of users who attempt to register using the different authenticating models (Shield-1(366), MP (331), TP (497) and Shield-2(392)).

During the login phase, the following accounts were captured: Shield-1 (1284), MP (2016), TP (1091) and Shield-2 (1273). Statistical record shows that 918 users who made used of Shield-1 did not register but tried to login. Similarly, 1685 users for MP tried to login without registering first. Also for TP, 594 participants who did not register, tried to login. In the case for Shield-2, 881 participants did not register but also attempt to login.

Users passwords also revealed that some users tried to log into the site without first registering, some others registered but at no time logged into the site, some during registration provided wrong passwords and never bothered to login, several others never accessed the website for training and so provided incorrect authenticating details and wrong passwords, consequently only the passwords of users who registered correct

authenticating details and logged into the site correctly/incorrectly using any of the authenticating models are considered for assessment. Therefore a total of 1092 accounts of users who made use of all four authenticating models are used for the study (i.e. Shield-1 (273), Shield-2 (273), TP (273) and MP (273)), which is actually about 85% of users' registration accounts.

In comparison, from a web study conducted on users multiple graphical passwords, Moncur and Leplâtre (2007) used only 35% of the users' password accounts generated due to nonconformities of password policies out of 172 who participated in the study. Everitt, et al. (2009) carried out a web study were 110 participants responded, however, only 100 participants account was focused on out of which only 60% responded to all the email-based prompt required. Zhang, et al. (2009) utilized only 93 students to participate in a password authentication experiment due to the fact that participants were restricted to those who participated in stage one and stage two of their experiment.

Method of Data Analysis

Percentages were used in the analysis of users authentication data to evaluate the ease at which users utilize the four models to access online materials by means of the following five complimentary measures: registration success rate (by noting the number of attempts required for successful registration authentication via help count), login success rate (by noting the number of attempts required for successful login authentication via help count), total success rate, registration time and login time.

Success rate of registered users of each model is calculated as the number of trials completed without errors or restarts over the total number of trials. To avoid misrepresenting the success rates "per trial", a password was considered successful only if entered correctly on the first attempt, (memorability test), with no restarts or errors. Failed registration and login attempts (where users pressed the submission buttons and were explicitly told that their passwords were incorrect) are classified with the restart counts since eventually both failed attempts and restarts are considered incorrect entries and unsuccessful. Success rate of all attempts to login is computed as the number of successful login over the total attempts to login for each model. Success rate of registered users is computed as the number of successful login over the total number of successful registered users.

The registration time measures the password registration or creation time (duration in minutes) while the login time measures the time to successfully login (duration in minutes). It began when the login screen is uploaded and continued until the user clicks the submit button to either login successfully or unsuccessfully irrespective of inherent errors.

To ascertain users' retention challenges, password memorizing was measured longitudinally twice: registration session (M1) (after filling the online questionnaire) and subsequent login (M2) within the duration of the study. In the retention trial users enter their passwords correctly one time. If a user entered an incorrect password, the system gives feedback that the password was wrong and the participant can reregister new credentials again.

For the number of incorrect submissions, all four models were measured and analyzed using Two-way Analysis of Variance (ANOVA). The between-subjects factor was the mode of authentication (i. e Shield-1, MP, TP, Shield-2) while the within-subjects factor was password credential retention (i. e. M1 and M2).

The following null hypotheses were posited for incorrect submissions:

$H_{0(1)}$: Trial will have a significant effect on participants incorrect retention submissions in all four models.

$H_{0(2)}$: Mode will have a significant effect on participants incorrect retention submissions in all four models.

$H_{0(3)}$: Trial and Mode interaction will have a significant effect on participants incorrect retention submissions in all four models.

The following null hypotheses were posited for correct retention submission time:

$H_{0(1)}$: There is a significant difference in the between-subjects factor (i.e. Shield-1, MP, TP, and Shield-2 retention submission time

Research Model

An on-going study website called Info Hub & Center accessible at http://secure-shield.com was developed that contains four different authentication models links: Shield-1 (exclusively a GP model), Shield-2 (a fingerprint biometric model), TP model and MP model. The website has three randomized interfaces with the exact same sets of links, one (see Figure 1 for one of the site interface).

The frontend links includes: the Homepage which takes the user always to the first page that appears upon opening the Info Hub & Center web browser program, Resources which summarizes what the site has to offer, Contact Us which contains the contact address of the researchers, Scholarship news which notify users to register and login using any of the authenticating models to be able to access the site facility. This notification appears too for Job Vacancies and Course Tutorial downloads links.

Training is another link on the Frontend that is available for users to train with any of the four models (see Figure 2 for Shield-1 training interface). When users created their accounts, the passwords creation time (mins), number of attempts to successfully Create Password (help count), Number of failed attempt to successfully Create Password (password failure count) and information about successful or unsuccessful password creation attempts for each of the four models were tracked and stored by the software. When participants attempted to login to their created accounts, the time to successfully login (duration in mins), number of attempts to successfully login (help count), Number of failed attempt to successfully login (password failure count) and information about successful or unsuccessful login attempts for each of the four models were stored by the software.

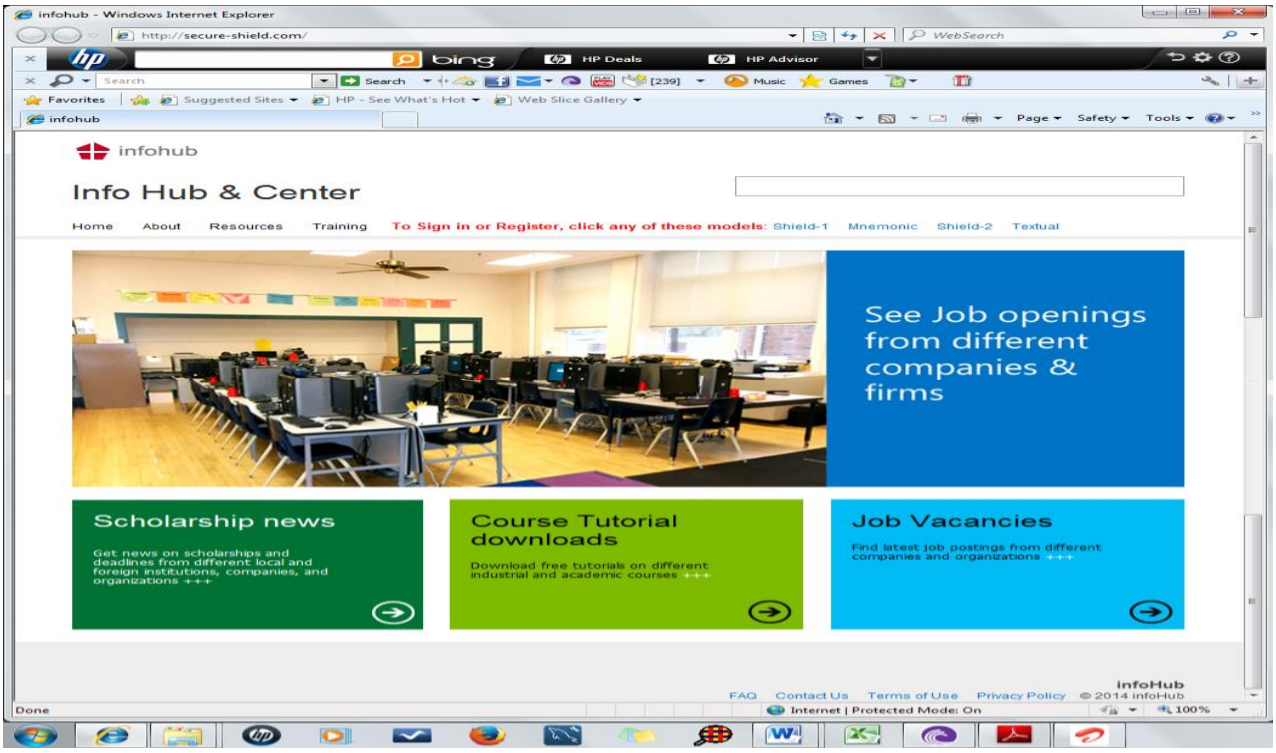

Figure 1: Website Homepage.

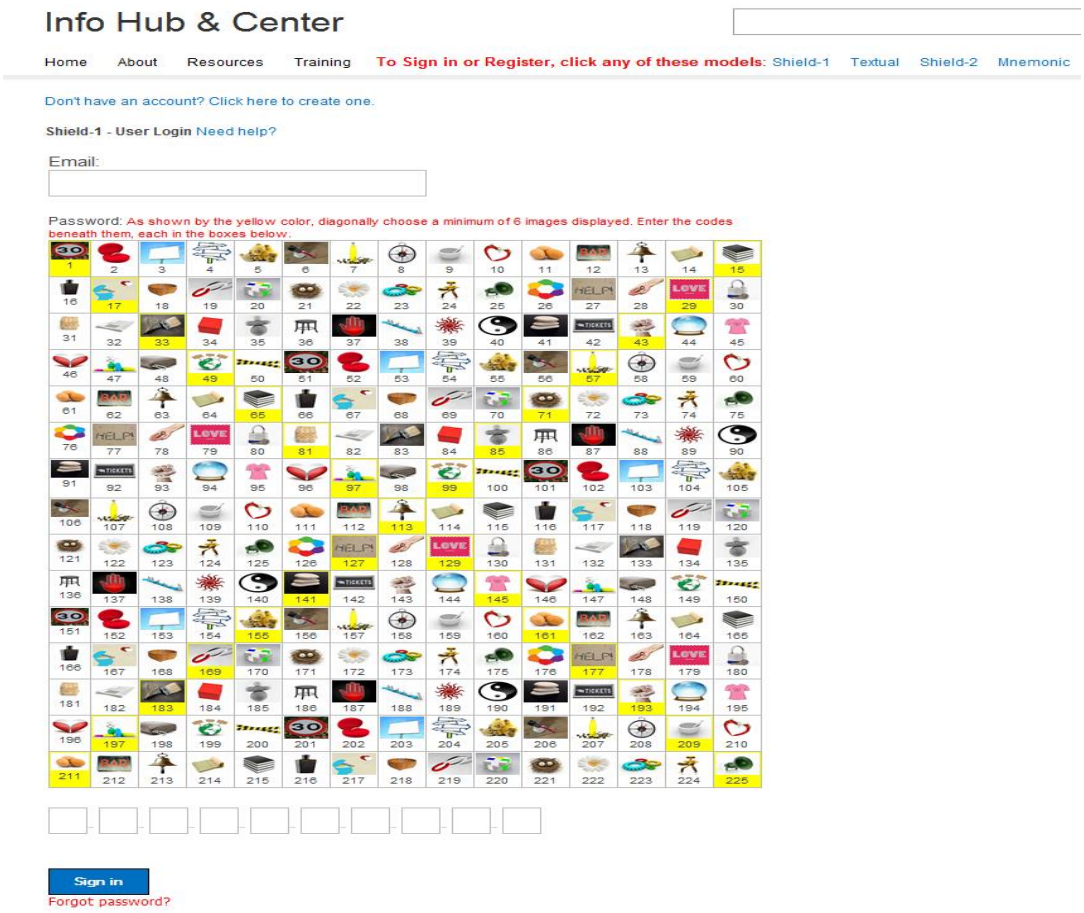

Figure 2: Shield-1 Training Interface.

RESULTS AND DISCUSSIONS

Success Rate

The success rates of the registration and login phases are shown in Table 2. The registration and login phase reports shows that users registering with Shield-1 performed better than those using Shield-2, MP and TP models. However, Shield-2 performed better than MP and TP models.

Users' registration for Shield-1 was 97% successful while MP had 91% success rate. TP had 93% and Shield-2 had 95%. In computing the success rate of all login attempts, it was evident that not all who login first registered, Shield-1 had 27%, MP was 14% login success rate, TP was 37% and Shield-2 was 28% login success rate, However during login, in computing the success rate of registered users, Shield-1 had 98% success rate, MP (92%), TP (87%) and Shield-2 (96%).

Registration and Login Time

The amount of time to register a valid password or login time was measured for only users who successfully registered or login (Table 3). It is certain that during registration, all four models falls within 63 seconds (the lowest recorded real time) and 402 seconds (the highest recorded time) (Valentine, 1998; Tari, et al, 2006). Shield-1 recorded the least login time of 40.8 seconds, followed by TP (82.2 seconds). Generally creating passwords or logging into the site using graphical images took a longer time than textual passwords.

However, a lot of users still had problems conforming to the rules of providing valid passwords, this can be observed from the highest recorded real time registered passwords, for Shield-1 it was 5.1mins. MP was 4.4mins, TP 3.5mins and Shield-2 6.7mins. Shield-1 recorded

the highest login time of 6.82mins and this is followed by Shield-2 (6.7mins).

Incomplete Retention Submission

Only credentials of users who registered and login subsequently making use of all four authenticating models were used for this study. Table 4 shows the results of the number of incomplete submissions.

Incorrect Retention Submission

The ANOVA results of the between-subjects factor (i.e. Shield-1, MP, TP, Shield-2) and within-subjects factor (i.e. M1 and M2) of retention trial lead us to refuse to reject $H_{0(1)}$ and conclude that trial have a significant effect on participants incorrect retention submissions in all four models. The F-value of 0.97 does not exceed the critical F-value of 3.782; $F(3, 1088) = 0.97$, $p < .01$.

Results of mode lead us to refuse to reject $H_{0(2)}$ and conclude that mode have a significant effect on participants incorrect retention submissions in all four models. The F-value of 1.39 does not exceed the critical F-value of 3.782; $F(3, 1088) = 1.39$, $p < .01$.

Results of Trial and Mode interaction lead us to refuse to reject $H_{0(3)}$ and conclude that trial and mode interaction have a significant effect on participants incorrect submissions in all four models.

Table 2: Comparison of Registration and Login Success Rates for the Four Authenticating Models.

Phase		Shield-1	MP	TP	Shield-2	Total
Registration	Attempt to Register	366	331	497	392	1586
	Success Rate	354 (97%)	301 (91%)	462 (93%)	371 (95%)	1488 (94%)
Login	Attempt to Login	1284	2016	1091	1273	5664
	Success Rate of all Attempt to Login	346 (27%)	277 (14%)	403 (37%)	356 (28%)	1382 (24%)
	Login Success Rate of Registered Users	346 (98%)	277 (92%)	403 (87%)	356 (96%)	1360 (91%)

Table 3: Comparison of the Mean (Standard Deviation) Time to Register/Login.

Models	Time to Register Password (mins)			Login Time (mins) (SD)		
	Lowest Time	Highest Time	Mean (SD)	Lowest Time	Highest Time	Mean (SD)
Shield-1	1.47	5.1	3.55 (1.01)	0.68	6.82	3.32 (1.40)
MP	1.73	4.4	2.45 (0.79)	1.73	5.07	2.27 (0.78)
TP	1.3	3.5	2.29 (0.99)	1.37	4.08	2.27 (0.78)
Shield-2	5.1	6.7	6.17 (0.62)	5.1	6.7	6.08 (0.66)

Table 4: ANOVA Summary Data for Incomplete Submission (Shield-1(273), Shield-2 (273), TP (273) and MP(273)).

		Shield-1	MP	TP	Shield-2
M1	M	0.19	0.24	0.38	0.10
	SD	0.4	0.54	0.67	0.3
	V	0.16	0.29	0.45	0.09
	SE	0.09	0..12	0.15	0.07
M2	M	0.10	0.14	0.24	0.14
	SD	0.3	0.48	0.54	0.36
	V	0.09	0.23	0.29	0.13
	SE	0.07	0.1	0.12	0.08
Total	M	0.14	0.19	0.31	0.12
	SD	0.35	0.51	0.6	0.33
	V	0.13	0.26	0.37	0.11
	SE	0.05	0.08	0.09	0.05

Where Mean is M, Standard Deviation is SD, Variance is V and Standard Error

The F-value of 0.34 does not exceed the critical F-value of 3.782; F(3, 1088) = 0.34, $p < .05$.

It is very interesting to note in this study that mode does have a significant effect on participants correct retention submissions in all four models. Participants were able to remember their passwords better using Shield-2 with only 0.12 incorrect submissions, this was closely followed by Shield-1 with 0.14 incorrect submissions; next was MP (0.19) and TP (0.31). This shows that participants have less retention challenges using the GP modes.

Correct Retention Submission Time

The ANOVA analysis of correct retention submission time is shown in Table 5. The test statistic is the F value of 6.55. Using α of .01, we have that $F_{01;\ 3,\ 1088} = 3.782$. Since the test statistic is much lower than the critical value, we accept the null hypothesis that there is a significant difference in the between-subjects factor (i.e. Shield-1, MP, TP, and Shield-2 retention submission time. The *p*-value for 0.000217 is 6.55, so the test statistic is significant at that level.

Results also show that: Shield-1 vs MP, Shield-1 vs TP, Shield-1 vs Shield-2 are significant at p<.01. However, MP vs TP, MP vs Shield-2 and TP vs Shield-2 are not significant. M1 phase was activated immediately after the training (learning) and 15-30 seconds distractor phase, thus participants had less difficulty recalling their passwords, irrespective of the mode of authentication during submissions. The lack of significant difference in the trial, mode and interaction between trial and mode of participants' incorrect submissions in all four models, indicate that a major factor that influenced the accuracy of password submission was password retention for all four model users. Participants correct retention submission time showed that MP was faster followed by TP, then Shield-1 and finally Shield-2.

CONCLUSION

We have presented the first study of multiple mode of authentication to methodically examine the effects of interference resulting from interleaving access to multiple mode of authenticating and the severity of users' memorability challenges. These effects have a number of significant implications for multimodal authentication model password usage. Generally, it is evident that users' behavior change as they try to get use to the models and accumulate passwords. Results of our web study indicate that for all four models registration rate, users' registration with MP performed better than that of the other three models while during the login phase, users performed better with Shield-2. The success rates of the registration and login phases reports shows that users registering with Shield-2 and Shield-1 performed better than those using MP and TP models. However, MP performed better than TP model. This is because users are provided beforehand with images that acted as cues during registration and many took advantage of these image cues during login. In these instances, the interference mitigating mechanism was effective.

Table 5: ANOVA Summary for Retention Submission Time (Shield-1(273), Shield-2 (273), TP (273) and MP (273)).

Source of Variance	Sum of Square (SS)	Degree of Freedom (df)	Mean Squares (MS)	F	P-value
Between Subjects	5.551	3	1.850	6.55	0.000217
Error	308.489	1088	0.282		
Total	314.040	1091			

The end result of the registration and login time reveals that a lot of users had problems conforming to the rules of providing valid passwords. This shows that users' time to authenticate can be significantly impacted by training, interference, familiarity and frequency of usage. Users with MP followed by Shield-1 and then Shield-2 took longer registration times, but as users get more familiar with the system, Shield-2 recorded the best login time followed by MP before TP and Shield-1. Thus in estimating registration and login the time for authentication models, design principles involving training, interference, familiarity and frequency of usage must be taken into consideration and incorporated.

The recall rate computed for participants who register with all four authenticating models but could not login at the end of the training (learning) session, after filling the questionnaire showed that users in the Shield-2 condition made significantly less recall errors when trying to recall their password. This proves that interference alleviation techniques are very helpful at aiding users to recall their passwords without adopting vulnerable habits. So in this research study, it is believed that memory cueing provided by images is at least part of the reason for enhanced users' password recall performance followed by familiarity based on frequent usage as is the case with TP passwords, which were the second best recalled passwords.

IMPLICATIONS AND FUTURE WORK

A major advantage of web studies is that large numbers of participants that are likely more diverse than in most controlled studies can be registered. Also, participants can be prompted to complete tasks at several different times, and participant's behavior may be more natural than in a laboratory setting making the studies very useful in an unsupervised environment (Everitt, et al., 2009; Moncur and Leplatre, 2007).

A major challenge is the fact that it is nearly impossible to determine if demographics information collected is accurate (Andrews et al, 2003; Florencio and Herley, 2007). However, additional ecological validity can be gained by integrating realistic tasks and systems, rather than using fabricated tasks.

As part of future work there is the need to determine users' password complexity and ascertain the persuasive elements that attracted Shield-1 images selections and that of Shield-2 against a particular fingerprint and verify if these elements will positively affect users MP and TP choices.

ACKNOWLEDGEMENT

We would like to acknowledge the National Information Technology Development Agency (NITDA) for supporting us financially with the research grant for this study.

REFERENCES

1. Adams, A. and M. Sasse. 1999. "Users Are Not the Enemy". *Communication of the ACM*. 42(12):41–46.

2. Alireza, P. and S. Angelos. 2008. "Universal Multi-Factor Authentication Using Graphical Passwords". Available at: www.computer.org/portal/web/csdl/doi/10.1109/SITIS.2008.92

3. Andrews, D., B. Nonnecke, and J. Preece. 2003. "Electronic Survey Methodology: A Case Study in Reaching Hard-To-Involve Internet Users". *International Journal of Human-Computer Interaction*. Lawrence Erlbaum Associates. 16 (2): 185–210.

4. Behzad, M., O. Mauricio, and E. Abdulmotaleb. 2008. "Novel Shoulder-Surfing Resistant Haptic-based Graphical Password". Available at: http://lsc.univ-evry.fr/~eurohaptics/upload/cd/papers/f119.pdf

5. Carstens D.S., L.C. Malone, and P. Mccauley-Bell. 2006. "Applying Chunking Theory in Organizational Password Guidelines". *Journal of Information, Information Technology, and Organizations*. 1, 97–113.

6. De Angeli, A., L. Coventry, G. Johnson, and K. Renaud. 2005. "Is a Picture Really Worth a Thousand Words? Exploring the Feasibility of Graphical Authentication Systems". *International Journal of Human-Computer Studies*. 63(1-2):128-152.

7. Everitt, K., T. Bragin, J. Fogarty, and T. Kohno. 2009. "A Comprehensive Study of frequency, Interference, and Training of Multiple Graphical Passwords". In: *ACM Conference on Human Factors in Computing Systems* (CHI).

8. Fernando, L., I. Podio, and J.S. Dunn. 2005. "Biometric Authentication Technology: From the Movies to Your Desktop". Available at: http://www.biometrics.org/

9. Florencio, D. and C. Herley. 2007. "A Large-Scale Study of Web Password Habits". *Proceedings of the International Conference on World Wide Web,* (WWW 2007), 657-666.

10. Fraser, N. 2006. "The Usability of Picture Passwords". Retrieved March 20 2006 from http://www.tricerion.com/files/285_Usability_of_picture_passwords.pdf

11. Goldstein, E. 2006. *Cognitive Psychology.* Wadsworth Publishing: London, UK.

12. Jain, A., R. Bolle, and S. Pankanti. 1999. "Introduction to Biometrics". In: *Biometrics: Personal Identification in Networked Society*. A.K. Jain, et al. (eds.): Dortrecht: London, UK. 1- 41.

13. Moncur, W. and G. Leplâtre. 2007. "Pictures at the ATM: Exploring the Usability of Multiple Graphical Passwords". *Proceedings of SIGCHI Conference on Human Factors in Computing Systems*. (887-894). Available at: http://www.academia.edu/318854/Pictures_at_the_ATM_Exploring_the_Usability_of_Multiple_Graphical_Passwords

14. NIST. 2002. *NIST report to the United States Congress, Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability*. Available at: *ftp://sequoyah.nist.gov/pub/nist_internal_reports/NISTAPP_Nov02.pdf, November 2002.NIST Special Publication 800-63*.

15. O'Gorman, L. 2003. "Comparing Passwords, Tokens, and Biometrics for User Authentication". *Proceedings of the IEEE*. 91(12).

16. Onibere, E.A. and A.O. Egwali. 2011. "An Empirical Analysis of Regular and Mnemonic Passwords". *Nigerian Journal of Applied Science.* 29: 52 – 57.

17. Pankanti, S., S. Prabhakar, and A.K. Jain. 2002. "On the Individuality of Fingerprints". *Transactions on PAMI*. 24(8): 1010–1025.

18. Ratha, N., J. Connell, and R. Bolle. 2001. "Enhancing Security and Privacy in Biometrics-Based Authentication Systems". *IBM Systems Journal*, 40(3):614– 634.

19. Scheuermann, D.M., S. Schwiderski-Grosche, and B. Struif. 2002. "Usability of Bometrics in Relation to Electronic Signature". EU-Study 502533/8, Darmstadt, Germany. http://www.sit.fraunhofer.de/english/SICA/sica_projects/project_pdfs/eubiosig.pdf

20. Tari, F., A. Ozok, and S. Holden. 2006. "A Comparison of Perceived and Real Shoulder-Surfing Risks between Alphanumeric and Graphical Passwords". In: *Proceedings of the Second Symposium on Usable Privacy and Security*. Pittsburgh, PA. July 12 – 14, 2006. SOUPS'06, 149. ACM: New York, NY, 56 – 66.

21. Valentine, T. 1998. "An Evaluation of the Passface Personal Authentic System". Technical report, Goldsmiths College, University of London: London, UK.

22. Wiedenbeck, S., J. Waters, J. Birget, A. Brodskiy, and N. Memon. 2005. "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System". *International Journal of Human-Computer Studies*. 63(1-2):102–127.

23. Yan. J., A. Blackwell, A. Anderson, and A. Grant. 2000. "The Memorability and Security of Passwords: Some Empirical Results". Technical Report No. 500. Computer Laboratory, University of Cambridge: London, UK.

24. Zviran, M. and Z, Erlich. 2006. "Identification and Authentication: Technology and Implementation Issues. *Communications of the Association for Information Systems*. 17(1): 90–105.

ABOUT THE AUTHORS

Annie Oghenerukevbe Egwali, is a Senior Lecturer at the Faculty of Physical Sciences, University of Benin. Benin City. Nigeria. She holds a Ph.D. degree in Software Engineering from the University of Benin. She is a member of the Nigeria Computer Society (NCS), Institute of Electrical and Electronics Engineers (IEEE), International Network for Women Engineers and Scientists (INWES), Third World Organizations of Women Scientists (TWOWS), National Association for the Advancement of Knowledge (NAFAK) and Nigerian Association of Educationists for National Development (NAEND). Her area of interests includes information technology, software engineering, gender studies, E-commerce, fuzzy systems, and software security. To date, she has supervised several undergraduate and postgraduate students.

Professor Emmanuel Amano Onibere, started his teaching career in the University of Ibadan in 1976 as an Assistant Lecturer. He moved to University of Benin in 1977 as Lecturer II. He rose to Associate Professor of Computer Science in 1990. In January 1999 he took an appointment

at the University of Botswana, Gaborone to provide academic leadership, while on leave of absence from the University of Benin. In October 2000, he was appointed Commonwealth Visiting Professor of Computer Science at the University of Buea in Cameroon to again give academic leadership. He returned in December 2002 to University of Benin. In 2003 he was appointed full Professor of Computer Science at the University of Benin.

Prof. Onibere, has been an External Examiner at the B.Sc., M.Sc., and Ph.D. levels in many Universities. He has been a resource person in a number of workshops and conferences both inside and outside Nigeria. He has a B.Sc. in Mathematics, and an M.Sc. and a Ph.D. in Computer Science. His special area of research is in software engineering. He has been involved in a number of research projects both in Nigeria and outside Nigeria. He has been Chairman of organizing committee of a number of conferences and training programs. Prof. E.A. Onibere has produced five Ph.D. and over 42 Masters graduates. He has published 5 books and fifty articles. He was formally the Deputy Vice Chancellor (academic) of University of Benin.

SUGGESTED CITATION

Egwali, A.O. and E.A. Onibere. 2016. "Memorability Interference Level for Multiple Modes of Authentication". *Pacific Journal of Science and Technology*. 17(2):122-133.