Evaluation of a Usable Hybrid Authentication System

Ayannuga Olanrewaju O.
Dept. of Computer Technology
School of Technology
Yaba College of Technology,
Yaba, Lagos, Nigeria.

Folorunso Olusegun
Dept. of Computer Science
College of Natural Science
University of Agriculture
Abeokuta, Nigeria.

Akinwale Adio T.
Dept. of Computer Science
College of Natural Science
University of Agriculture
Abeokuta, Nigeria.

ABSTRACT
The increase in the use of automated systems has brought about an increase in the amount of personal information in electronic form; and as a result there is need for confidentiality. A good system must be able to identify "who" is accessing "what". Several authentication systems use password (text) as an authentication means while in modern computing, graphical password is beginning to gain ground due to its advantage in the area of usability. This paper studies graphical password with the view of merging its strength with the strengths of text password to produce what is known as a hybrid authentication system.

General Terms
Usable Secure System

Keywords
User Authentication, Graphical Password, Usable Security.

1. INTRODUCTION
With the reduction in the cost of acquiring computer system and huge advancement in the use of computer in many applications such as data transfer, sharing data, login to e-mail or Internet, there is increase in the number of users, which implies increase in data stored in our database. This poses a challenging task for system and network administrators to determine user authentication. **Authentication** has been the catalyst for business organization in information protection and **security**. Wiedenbeck et al (2005) stated that authentication is the process of determining whether a user should be allowed access to a particular system or resource. Richard (2001) opined that authentication is the process of verifying the identity of a certain person. User authentication involves issues of both usability and security; too often one or the other is ignored even when it is clear that both are important and necessary.

IT security could be enhanced by using multiple methods to authenticate users, such as combining "something you know" (e.g., a password) with "something you have" (e.g., a smartcard or token) and "something you are" (e.g., a biometric characteristic). Although the use of biometrics and smartcards is growing, passwords are still the most common, and sometimes the only authentication mechanism used by many organizations. Therefore, it is important to find ways to improve password effectiveness.

2. BACKGROUD
Users tend to pick short passwords or passwords that are easy to remember, which makes the passwords vulnerable for attackers to break. Furthermore, textual password is vulnerable to shoulder-surfing, hidden camera and spyware attacks. Graphical password schemes have been proposed as a possible alternative to text-based scheme. However, they are mostly vulnerable to shoulder-surfing too.

Security and usability are often viewed by security experts as opposite extremes, and one must necessarily be sacrificed for the other. While alternative authentication mechanisms such as biometrics (Jain, Hong and Pankanti, 2000) are widely known, these have their own security, privacy, and usability problems that limit their use to specific applications. Due to their widespread usage and relatively low cost, knowledge-based schemes such as passwords are unlikely to disappear; and they may well become even more popular as more day-to-day tasks are computerized.

For an authentication mechanism to be secure, it must be undisclosed, abundant and predictable (Renaud, K., & Smith, E., 2001). The security of a password can be rated for the ability of a potentially malign user to observe the code (observability), guess the code (guessability) and record the code (recordability) (DeAngeli, A. et al, 2005).

3. GRAPHICAL PASSWORDS
For over a century, psychology studies have recognized the human brain's superior memory for recognizing and recalling visual information as opposed to verbal or textual information (Chiasson, 2008). The most widely accepted theory explaining this difference is the **"dual-coding theory"** (Paivio, 2006), suggesting that verbal and non-verbal memory (i.e., word-based or image-based) are processed and represented differently in the mind.

Graphical passwords are intended to capitalize on this human characteristic in hopes that **by reducing the memory burden** on the user, **more secure** (e.g., longer or more complex) passwords can be produced and users will not resort to unsafe practices in order to cope (Jermyn et al, 1999; Monrose and Reiter, 2005). Graphical passwords can be categorized into ***Pure Recall, Cued Recall and Recognition.*** .

3.1 Pure Recall
Graphical passwords requiring pure recall are most similar to text passwords because users must remember their password and reproduce it without any cues from the system. Examples include:

- **Draw-A-Secret (DAS)**

With DAS users draw their password on a 2D grid using a stylus or mouse as shown below (figure 1). The password is composed of the coordinates of the grid cells that the user passes through while drawing. A drawing can consist of one continuous pen stroke or several strokes. To log in, users repeat the same path through the grid cells. The theoretical password space is determined by the coarseness of the

underlying 2D grid and the complexity of the images. A coarser grid helps with usability, while a finer grid increases the size of the password space.

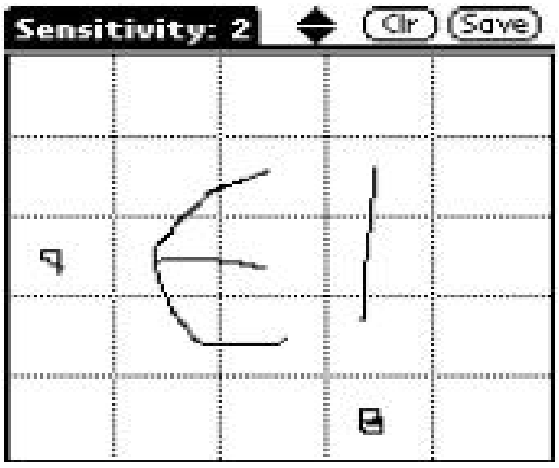

Figure 1: Sample Draw-A-Secret password (Adapted from Jermyn, Mayer, Monrose, Reiter, and Rubin, 1999)

- **Pass-Go**

Tao's Pass-Go was named for the Chinese board game of Go which consisted of strategically placing tokens on the intersections of a grid. In Pass-Go as shown below (figure 2), users draw their password on a grid, except that the intersections are used instead of grid squares. Visually, the user's movements are snapped to grid-lines and intersections so that the drawing is not impacted by small variations in the trace. Users can choose pen colours to increase the complexity of their drawing.

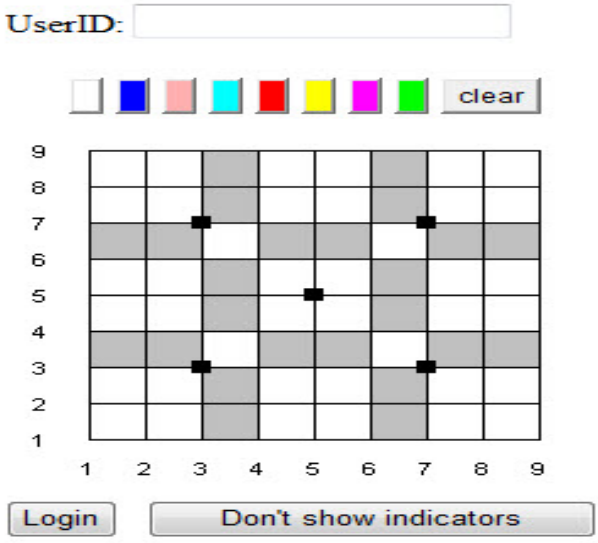

Figure 2: Login screen for Pass-Go (adapted from Tao H. and Adams C, 2008)

3.2 Cued Recall

In cued-recall systems, the system provides a cue to help trigger the user's memory of the password (or portion thereof). This feature is intended to reduce the memory load on users and is an easier memory recall task than pure recall. Some examples of the cued-recall system are:

- **Inkblot Authentication**

Although not strictly a graphical password system, Inkblot Authentication as shown below (figure 3) uses images as a cue for text password entry. The system presents computer generated "inkblots" and users respond by entering text characters that match those earlier selected when the password was created. During password creation, users are shown a series of inkblots and asked to type in the first and last letter of the word/phrase that best describes the inkblot. These pairs of letters become the user's password. The inkblots are displayed, in order, as cues during login and users must enter each of their 2-character responses. The authors suggest that with time, users would memorize their password and would no longer need to rely on the inkblots as cues.

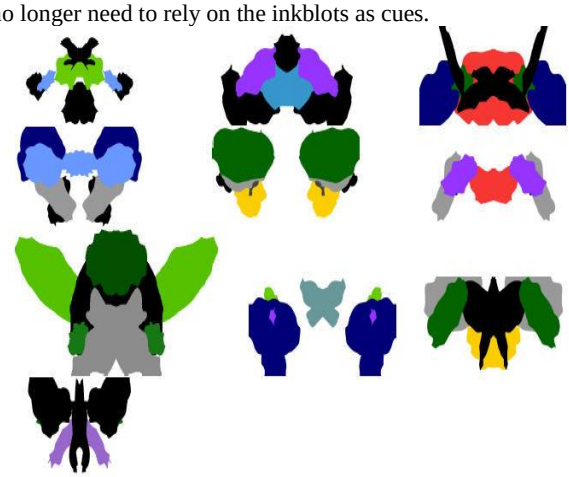

Figure 3: Inkblots used in the Inkblot Authentication user study (adapted from Stubbleffeld A. and Simon D., 2004)

- **Blonder's Graphical password**

Blonder (1996) was the first to propose click-based graphical passwords. In his scheme, a system administrator prepares an image by defining the perimeter of objects within the image ("tap regions"), typically along the outlines of the objects in the scene. Users select a sequence of these pre-defined objects as their password by clicking on each object. For example, in Figure 4, a password could consist of clicking on the pocket watch, the red bead necklace, the picture on the wall, the watch on the bed, and the camera. To log in, users click on each object in the same order. The image is intended as a cue to help users remember their password.

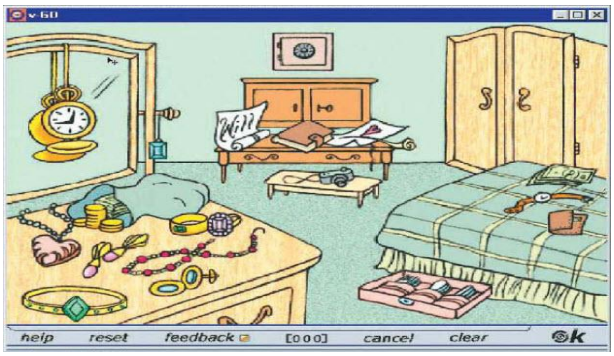

Figure 4: Passlogix implementation of Blonder's graphical passwords. (Adapted from Suo X., Zhu Y., and Owen G., 2005)

3.2.1 Recognition based

Several theories exist to explain the difference between recognition and recall memory, based on whether these are

two unique processes or whether they are similar and differ only in their retrieval difficulty (Anderson and Bower, 1972). It is generally accepted, however, that recognition is an easier memory task than recall (Kintsch, 1970). In recognition-based graphical password systems, users typically memorize a portfolio of images during password creation and then must recognize their images from among decoys to log in. examples of graphical password schemes in this category include:

- **Deja Vu**

In Deja Vu, users select and memorize a subset of images from a larger sample to create their portfolio. To log in, users must recognize images belonging to their pre-defined portfolio from a set of decoy images; in the test system, a panel of 25 images is displayed, 5 of which belong to the user's portfolio. Users must identify all the images from their portfolio and only one panel is displayed. Images of "randomart" are used to make it more difficult for users to write down their password or share it with others by describing the images from their portfolio. The authors report that a fixed set of 10000 images is sufficient, but that "attractive" images should be hand-selected to increase the likelihood that images have similar probabilities of being selected by users.

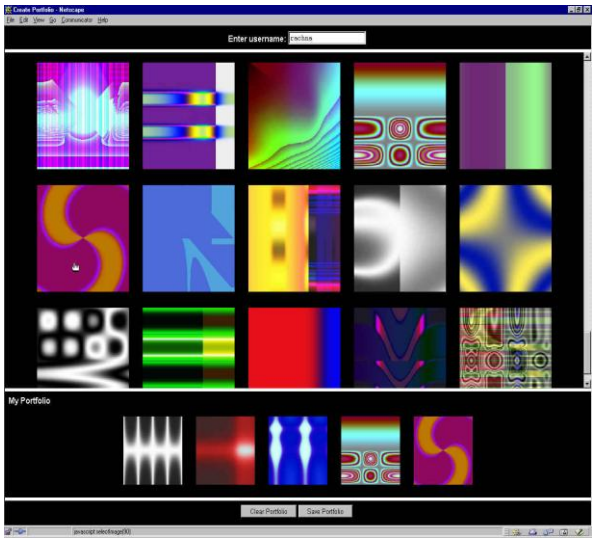

Figure 5: Screenshot of the Déjà vu graphical password system (adapted from Dhamija. and Perrig, 2000)

- **Jetafida scheme**

In 2008, this model is proposed based on trying to gather all the usability features, like ease of use, easy to create, easy to memorize, easy to learn and acceptable design and layout in one algorithm. According to the diagram below (figure 6), during registration, the user will select three pictures as a password and then sort them according to the way he wanted to see them in login phase.

Jetafida scheme stands out from other Recognition-Based Graphical User Authentication Algorithms due to its usability features as well as security technique. It has the same usability feature based on the ISO's standard when compared with picture password scheme as they are both efficient.

Figure 6: Jetafida scheme (Adapted from: "Graphical password: prototype usability survey, Ali Mohamed, E., Norafida. I.," 2008)

.

3.3 Hybrid Authentication System

The method we propose combines a traditional text-based password with a graphically-based scheme. The notion for using such a scheme is to attempt to maximize both the security of the authentication process and extent to which the login requirements are memorizable to the user.

The new system was designed with enhanced security and usability features. The concept of distributed security is implemented in the two-step click-based authentication process. The proposed system implements the message digest 5 algorithm for the encryption of the text password involved in the authentication process. All encrypted text passwords are stored in a database different from the one in which all graphical images are stored; meaning that the databases have been distributed.

As a security feature, all text passwords will not be decrypted at any time, that is, only cipher-text without a decryption key will be involved in the whole process. This denies the administrator from gaining access to other user accounts as he will not be able to decode the content on the database even if he views it. Also, with the use of AJAX technology, all images are loaded and refreshed on one page without changing the web address therefore making it impossible to trace the location of all images from a web browser (address bar or status bar).

The research within this paper looks at how a hybrid system for authentication can be efficient security-wise and also satisfy usability requirements.

4. STUDY

Can the use of a hybrid authentication system satisfy both usability and security? How many people will support that the hybrid system is usable and yet secure?
In a study carried out by Wendy Moncur and Grégory Leplâtre in 2007, it was established that graphical passwords represent a valuable solution to the usable security problem caused by the multiplication of passwords.

4.1 Methodology

A total of two hundred computer users from different higher institution in Lagos state volunteered to take part in the experiment. They used the system for a period of three weeks and at random, one day of each week was used to monitor their performance on the system.

The system allows users to supply a username and choose from a grid of thirty, three images which will serve as their pass-image. The system generates a four-digit text password for each user and demands that both the text password and the pass-images coupled with their username are supplied, in other to login.

The pass-image selection interface is shown below (figure 7).

Figure 7: Image selection interface of the hybrid system.

At the end of the experiment, questionnaire was given to each of the persons that partook in the experiment and the result was collated and analyze.

5. RESULS

The analysis was based on the usability requirements of the ISO standard. These are efficiency, effectiveness and satisfaction. For effectiveness, the following statistics was gathered (Table 1).

Table 1: Table showing frequency and percentages of users opinions on system effectiveness.

Frequency Table				
	Freq	%	Valid %	Cumm %
Strongly Agree	107	53.5	53.5	53.5
Agree	78	39.0	39.0	92.5
Disagree	15	7.5	7.5	100
Total	200	100	100	

Figure 8 is a pie chart showing the percentages of user opinions on the systems effectiveness.

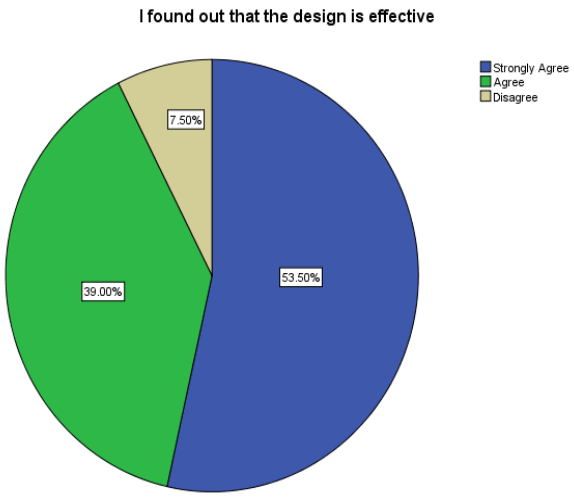

Figure 8: Pie chart showing users perception on effectiveness

Also, in the area of efficiency, the table below (Table 2) shows figures gathered from the analysis of data collected from user opinions on how efficient the system is.

Table 2: Table showing frequency and percentages of users opinions on system efficiency.

Frequency Table					
		Freq	%	Valid %	Cumm %
Valid	Strongly Agree	109	54.5	54.5	54.5
	Agree	80	40.0	40.0	94.5
	Disagree	11	5.5	5.5	100
	Total	200	100	100	

Figure 9 is a pie chart showing the percentages of user opinions on the systems efficiency.

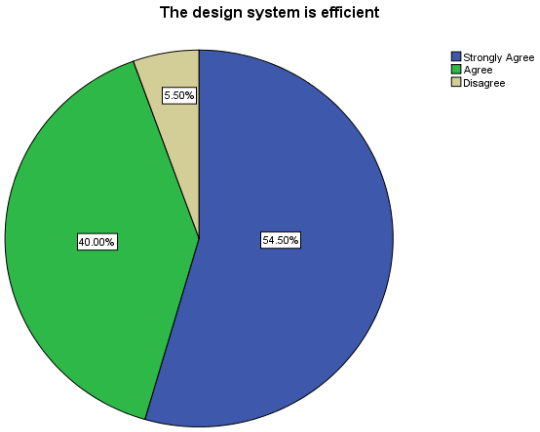

Figure 9: Pie chart showing users perception on efficiency

5.1 Security Assessment

The hybrid system seeks to find a balance to security and usability by combining the usability strength of graphic password and the security of encrypted system generated text password.

The security of the system is assessed by subjecting it to some hacking techniques. Dictionary attack as well as brute force attack was used in attempt to extract the text password supplied by the user. Since the text password was system generated as well as encrypted, it was not revealed by any of the hacking technique used. Further attempt made to get the text password by advance hacking tools proved non-productive as only cipher-text was found and will take a very long time to crack due to high entropy.

6. CONCLUSION

This study has demonstrated the use of hybrid authentication as an alternative authentication scheme. It revealed that combining both text and graphics improves on the security at the same time usability of an authentication system. It would be of interest to repeat the study with larger sample sizes. Graphical password studies so far have consistently used small sample sizes, a failing identified by Suo et al (2005).

7. REFERENCES

[1] Wiedenbeck S., Waters J., Birget J, Brodskiy A., and Memon N. (2005). Authentication using graphical passwords: Basic results. In 11th International Conference on Human-Computer Interaction (HCI International).

[2] Richard E. Smith. October 2001. Authentication: From Passwords to Public Keys, chapter 2-3,6, pages 39{101, 155{192. Addison-Wesley Professional.

[3] Jain A, Hong L., and Pankanti S. February 2000. Biometric identification. Communication of the ACM, 43(2):91 -98.

[4] Renaud, K., & Smith, E. (2001). Jiminy: helping users to remember their passwords. In Proc. SAICSIT Annual Conference.

[5] DeAngeli, A., Coventry, L., Johnson, G., & Renaud, K.(2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 63(2005), 128-152.

[6] Chiasson S., Forget A., Stobert E., van Oorschot P., and Biddle R. September 2008. Multiple password interference in text and click-based graphical passwords. (Manuscript under submission). Technical Report TR-08-20, School of Computer Science, Carleton University.

[7] Paivio A. 2006. Mind and its evolution: a dual coding theoretical approach. Lawrence Erlbaum: Mahwah, N.J..

[8] Jermyn I., Mayer A., Monrose F., Reiter M., and Rubin A. August 1999. The design and analysis of graphical passwords. In 8th USENIX Security Symposium.

[9] Tao H. and Adams C. 2008. Pass-Go: A proposal to improve the usability of graphical passwords. International Journal of Network Security, 7(2): 273-292.

[10] Stubblefield A. and Simon D. (2004). Inkblot Authentication, MSR-TR-2004-85. Technical report, Microsoft Research, Microsoft Corporation.

[11] Blonder G. (1996). Graphical passwords. United States Patent 5,559,961.

[12] Suo X, Zhu Y, and Owen G. December 2005. Graphical passwords: A survey. 21st Annual Computer Security Applications Conference.

[13] Anderson J. and Bower G. March 1972. Recognition and retrieval processes in free recall. Psychological Review, 79(2):97.

[14] Kintsch W. (1970). Models for free recall and recognition. In D. Norman, editor, Models of human memory, chapter Models for free recall and recognition. Academic Press: New York.

[15] Dhamija, R. and Perrig, A. (2000). Deja Vu: A User Study Using Images for Authentication. In Proceedings of the 9th USENIX Security Symposium. http://www.simson.net/ref/2000/usingImagesForAuthentication.pdf>. 45–48.

[16] Ali Mohamed Eljetlawi and Norafida Bt.Ithnin. (2009). Graphical Password: Usable Graphical Password Prototype. Journal of International Commercial Law and Technology. Vol. 4, Issue 4

[17] Wendy Moncur and Grégory Leplâtre (2007): Pictures at the ATM: Exploring the usability of multiple graphical password.