Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY
Vol. 10. No. 2, June 2022

Article Citation Format
ADEBIMPE, Lateef Adekunle (2022):
VPass: Graphical Password Authentication Using Vowels.
Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology. Vol. 10 No. 2. Pp 93-99
DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V10N2P5

Article Progress Time Stamps

Article Type: Research Article
Manuscript Received: 18th Feb, 2022
Review Type: Blind
Final Acceptance:: 12th March, 2022
Published: 2nd June, 2022

VPass: Graphical Password Authentication Using Vowels

ADEBIMPE, Lateef Adekunle
Department of Computer Science
Emmanuel Alayande College of Education
Oyo, Oyo State, Nigeria.
E-mail: dradebimpela@yahoo.com

ABSTRACT

Information is a great asset in the modern society. Information and Communication Technology has undoubtedly provided great access to knowledge and information. However, unauthorized access to sensitive information has posed serious danger to individual and corporate organizations. Therefore, information security became a necessity to protect confidentiality of sensitive information. Information security ensures authentication (proving to be genuine) of users so that only authorized users can access a secured system. Authentication methods are used to protect classified information. The commonest form of authentication method is alphanumeric password. Complex (strong and random) alphanumeric password is difficult for users to remember, as a result of this, users are usually tempted to use weak (easily guess) alphanumeric password. Consequently, graphical password was invented to overcome the problem associated with alphanumeric password. Graphical password is a form of authentication that uses visual objects. Human brain can remember pictures better than sequence of alphanumeric characters. The proposed graphical password authentication scheme VPass, adopts the concept of English vowels. In the proposed graphical authentication scheme, VPass, a user is only required to remember a registered location from a challenge set consisting 5x5 grid cells. Therefore, VPass, proffers solution to memorability issue.

Keywords Graphical Password, Visual Object, Image, Alphanumeric, Authentication, Challenge Set.

1. INTRODUCTION

In information security, authentication is a very significant tool for the verification of identity [1]. Authentication ensures that a user is who he/she claims to be. Authentication is used to determine whether a user should be given access to a system. Graphical password is an authentication method

where a user selects visual objects (e.g. images, pictures, icons) from one or more challenge sets in a specific order. Researches have shown that many graphical password schemes have been proposed [1,2]. However, in most of the existing graphical password schemes, the complexity meant to prevent attackers from gaining access often lead to memorability issue and thereby resulted to high authentication failure by the legitimate users. Therefore, in this research, a new graphical password method is proposed to aid memorability.

2. RELATED WORKS

Nizamani et al. proposed GPass in 2016 [3]. During the registration process, a user is required to register a username, if the username is already present in the system, the user would be required to enter another username. After that, the user is required to register password of minimum of five characters, which can be either alphanumeric, graphical or the combination of both. During authentication, a user is required to enter registered username. After that, a dialog box consisting of alphanumeric characters and pictures is shown. Both alphanumeric characters and pictures are categorized into different groups. To login, a user is required to click the group where the first character of the registered password is shown. The user needs to repeat this process by clicking on the groups displaying each of the characters of the registered password one by one.

In the TrimT proposed by Adebimpe in 2020 [4], a user is required to register several images from the images shown in the grid during the registration process. After that the user is required to reconfirm the registered images. During the authentication process, the user is required to identify the row without registered images in a challenge set of 5x5 grid consisting twenty five (25) images randomly displayed. To login, the user is required to click the row without a registered image. In the graphical authentication scheme proposed by Abdalkareem et al in 2021 [5], a user is required to register username. After that, an image is shown. The user is required to register a starting point by clicking on the desired point in the displayed image. After that the user is required to move the mouse toward a desired direction on the image to create a password path. Difference in variant locations is recorded and establish where the path should pass through to create the password. The user can use one of the specified locations to be authenticated. The user is required to confirm the password by repeating the mouse movement before saving it in the database. During the authentication process, the user is required to redraw the path inside the tolerance of their chosen pixels/points and also in the right sequence. The user is authenticated if the the drawing touches the identical pixels in the correct sequence.

Gopali et al proposed HyPA scheme in 2021 [6]. During registration, a user is required to register an email address. After that, a 3x3 grid consisting of images is shown. The user is required to register several images. For each of the registered image, the system prompt the user to augment it with alphanumeric password. During authentication, the user is required to provide the registered email address. After that, the user would be required to select registered images and enter appropriate alphanumeric password by following the sequence adopted during registration. Position of the images are randomly reshuffled after each click. In the graphical authentication scheme proposed by Khodadadi et al in 2021 [7], which focused on improving the usability of graphical passwords, pictures of prominent actors were used to aid memorability. During registration, a user is required to register at least six images and maximum of eight images from the images shown on 4x8 grid.

With maximum number of eight images in the spaces provided for drag and drop images, if a user decide to use six images, such user will have two spaces and the password of such user will be a mixture of six images and two spaces. The user is expected to arrange the images in a sequence (desired order) using drag and drop feature. Once the registration process is successful, a link is generated for the user to login, otherwise, a dialog box indicating registration failure is shown. During authentication, a user is required to identify and click the registered images in the sequence they were registered to login. Authentication is successful once this is done correctly. In the graphical authentication scheme proposed by Dias and Reeja in 2021 [8], a user is required to register several images. After that, the user is required to select a click point per image. The click point in the image will generate a tolerance area around the chosen click point based on the predefined radius. The number of points available to choose depend on the radius of the tolerance area. An offset is considered in an image on all the four edges. This offset is a non-clickable area which is defined based on the radius.

Rajarajan and Priyadarsini proposed a graphical password authentication scheme named SelfiePass in 2021 [9]. During registration, a user is required to register one image. The user may browse over the system gallery to select personally taken image. The users are advised to avoid using downloaded images. The belief is that images taken by the user are unique photo in the world and may not be available elsewhere in the world. Therefore, it would be impossible for attackers to reproduce such a unique image. Once the image has been selected, discretization lines are drawn over it. During authentication, the image is shown to the user with the grid lines drawn over it. The user is not expected to click on the points shown, rather the user task is to move the grid columns horizontally and vertically so as to position the secret token on the first click point. After that, the user enter the row and column information of the two click points. Authentication is successful if correct information is entered, otherwise, authentication failed and the user is asked to try again.

In the graphical paswword authentication scheme proposed in 2022 by Akter and Ashraf [10], a user is required to register an alphanumeric username. After that, the system automatically generates a unique 4-digit decimal key number for the user. The user needs to remember the unique 4-digit decimal key number. The username and the unique 4-digit decimal key number are encrypted using cryptography mechanism before they are eventually saved in the database. To login, a user is required to enter the username. If the username is correct, a 10x10 image grid is shown. The user is required to enter the unique 4-digit decimal key number by clicking on the image grid shown. Jijees et al proposed an authentication scheme named Passnumbers in 2022 [11].

During the registration procedure, a user is required to register a userID. After that, the user is required to register one image. The image is discretized into a 10x10 grid. After that, the user is required to select certain point (row, column) as password. The password consists of a set of numbers in a range between (0 to 99) each value includes two digits. The first digit in the pair is used to select the row and the second digit is used to select the column. During the authentication procedure, a user is required to enter userID. If the userID is correct, a 10x10 grid cell is shown. After that, the user is required to click the cell corresponding to the registered cell. The arrangement of numbers varies dynamically at each login process.

3. PROPOSED SYSTEM

The proposed system is divided into registration phase and authentication phase

3.1 Registration Phase

During the registration phase, a user is required to register one location from the locations shown in the 5x5 grid. The user is required to confirm the registered location. The registration is saved into the database once the registered location matches, otherwise an error message is displayed and the user is required to try again.

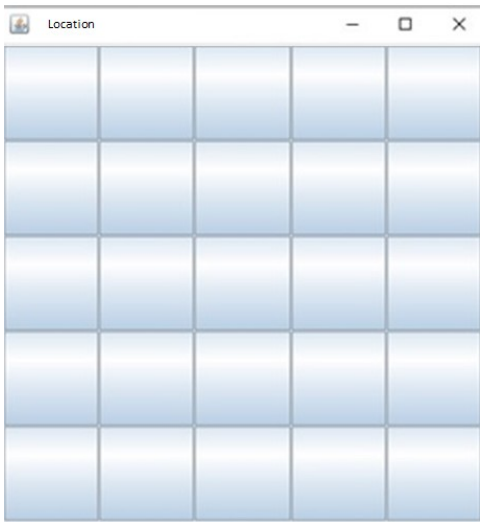

Figure 1: VPass Registration Phase

3.2 Authentication Phase

During the authentication phase, a challenge set that consists of 5x5 grid is shown. A total of twenty five (25) images consisting vowel letters are randomly displayed in the 5x5 grid cells. The user is required to identify the vowel shown in the registered location. To login, the user is required to type any word that consists of vowel shown in the registered location as pass. To ensure strong authentication, this process is repeated for three rounds.

For each round, the vowels shown in the grid are reshuffled using uniform randomization algorithm. Therefore, the vowel shown in the registered location may be differed and consequently the permissible word to be used as a pass will ultimately be different. To avoid guessing attack, the user will not be informed separately (for each of the rounds) whether the password is correct or incorrect. Authentication is only successful if a user is able to supply correct pass for the three rounds.

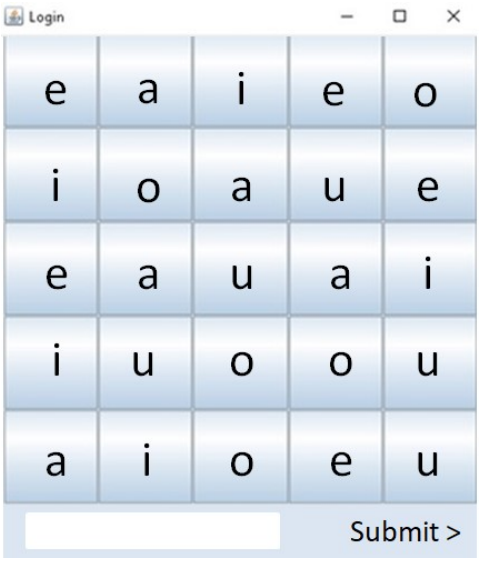

Figure 2: VPass Authentication Phase

4. EVALUATION

4.1 Participants

A total of 40 participants were invited to evaluate the effectiveness of the proposed method.

4.2 Procedure

A tutorial was conducted to train the participants on how to use the proposed system. During the tutorial, the participants were guided to create personal accounts and get familiar with the authentication process. After that, each of the participants was requested to login. The system automatically recorded the login time.

4.3 Results

38 (95%) of the participants were able to login successfully, 2 participants failed the authentication process. As shown in the table 1, participants recorded 3.0 seconds minimum login time. The maximum time taken by the participants for a successful login is 8.0 seconds. On the average, participants recorded 4.7 seconds login time.

Table 1: Successful login time

Item	Time (seconds)
Minimum	3.0
Maximum	9.0
Mean	4.7

5. DISCUSSION

Table 2: Login time Comparison

Method	Min login time (seconds)	Max login time (seconds)	Mean login time (seconds)
GPass [3]	No specify	No specify	24.7
TrimT [4]	2.0	4.0	2.3
Abdalkareem et al. [5]	No specify	No specify	No specify
HyPA [6]	2.7	3.5	No specify
Khodadadi et al [7]	No specify	No specify	No specify
Dias and Reeja [8]	No specify	No specify	11.0
SelfiePass [9]	No specify	No specify	No specify
Akter and Ashraf [10]	No specify	No specify	No specify
Passnumbers [11]	No specify	No specify	No specify
Proposed method	3.0	8.0	4.7

Table 2 shows the comparison of the successful login time between the selected graphical password authentication schemes and the proposed method. TrimT system [4] has the shortest minimum login time 2.0 seconds, followed by HyPA system [6] 2.7 seconds and the proposed method 3.4 seconds. The proposed method has the highest maximum login time 8.0 seconds, followed by TrimT system [4] 4.0 seconds and then HyPA system [6] 3.5 seconds. In term of mean login time, TrimT system [4] has the shortest login time 2.3 seconds followed by the proposed method 4.7 seconds, then Dias and Reeja system [8] 11.0 seconds and GPass system [3] 24.7 seconds.

6. FUTURE WORK

The user study conducted in this research examined the successful authentication and authentication failure. In other words, the user study focused on participants ability to login or not. Therefore, there is need to conduct more user study to evaluate the security and other usability factors.

REFERENCES

[1] Kaka, J.G., Ishaq, O.O., & Ojeniyi, J.O. (2021, February). Recognition-Based Graphical Password Algorithms: A Survey. *In 2020 IEEE 2nd International Conference on Cyberspac (CYBER NIGERIA)*, (pp. 44-51), IEEE.

[2] Chiasson, S., Van Oorschot, P.C., & Biddle, R. (2007, September). Graphical password authentication using cued click points. *In European Symposium on Research In Computer Security*, (pp. 359-374), Springer, Berlin, Heidelberg.

[3] Nizamani, S. Z., Hassan, S. R., & Khan, M. M. (2016). GPASS: A Graphical Password Scheme using alphanumeric characters and pictures. *International Journal of Computer Science and Information Security*, *14*(7), 251.

[4] Adebimpe, L.A. (2020). TrimT: A graphical password authentication scheme. *Journal of Advances in Mathematical & Computational Sciences*, 8(3), 1-12.

[5] Abdalkareem, Z. A., Akif, O. Z., Abdulatif, F. A., Amiza, A., & Ehkan, P. (2021, February). Graphical password based mouse behavior technique. In *Journal of Physics: Conference Series* (Vol. 1755, No. 1, p. 012021). IOP Publishing..

[6] Gopali, S., Sharma, P., Khethavath, P. K., & Pal, D. (2021, April). HyPA: A Hybrid Password-Based Authentication Mechanism. In *Future of Information and Communication Conference* (pp. 651-665). Springer, Cham.

[7] Khodadadi, T., Javadianasl, Y., Rabiei, F., Alizadeh, M., Zamani, M., & Chaeikar, S. S. (2021, December). A Novel Graphical Password Authentication Scheme with Improved Usability. In *2021 4th International Symposium on Advanced Electrical and Communication Technologies (ISAECT)* (pp. 01-04). IEEE.

[8] Dias, N., & Reeja, S. R. A Systematic approach towards enhancing of Security and usability of graphical password through cognitive computing and data mining..

[9] Rajarajan, S., & Priyadarsini, P. L. K. (2021, August). SelfiePass: A Shoulder Surfing Resistant Graphical Password Scheme. In *2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT)* (pp. 563-567). IEEE.

[10] Akter Sharna, S., & Ashraf Ali, S. (2022). Image Based Password Authentication System. *arXiv e-prints*, arXiv-2205.

[11] Jirjees, S. W., Mahmood, A. M., & Nasser, A. R. (2022). Passnumbers: An Approach of Graphical Password Authentication Based on Grid Selection. *Journal homepage: http://iieta. org/journals/ijsse*, *12*(1), 21-29.