Impact of Background Images on the DAS (Draw- A- Secret) Graphical Password Authentication Scheme

Y.D.S.Arya and Gaurav Agarwal
Invertis University, India

ABSTRACT
The basic idea of Draw- A Secret technique is that a user is asked to draw a simple picture on a 2D grid. The coordinates of the grid, occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. But sometimes user fails to recall his/her password during the registration process. In the proposed work we are applying A Background image with das scheme to increase the remembrance of passwords. The basic idea behind the scheme is that the human nature that he or she can recognize pictures easily then the 2 d grids.

General Terms Back ground images, Graphical password, Draw-a- Secret, Authentication

1-INTRODUCTION
It is very commonly existence of alphanumeric passwords for use authentication as it was not so much secure for the users so the enhancement occurred in the form of graphical passwords. Many people find it difficult to remember password, and they tend to choose easily passwords. Many of the decencies of textual passwords arise from the limitation of human memory[4].Graphical password can be categorized in to two parts that is recognition based and recall based.[1]. Das scheme comes under the recall based technique in which user's password is free-from drawing from produced on an NXN grid. This technique is alphabet independent [2]. Das has some features like it has the larger password space larger than the textual schemes. Second advantage is that it is not only use for user authentication but the technique can also be used for the cryptographic key generation. In this paper we are presenting the new approach for the DAS with the help of background image. The implementation of background image will be useful for the users to remember their passwords generated by the DAS technique, a user will first choose a background image to be overlaid by the grid, and then draw their secret as in DAS. Background image would encourage users to choose more complicated passwords, which are usually less [8].

Vulnerable to dictionary and other guess attacks also this will help user to memorize their passwords. In our study result shows that user using background images for DAS can set less predictable but more complicated passwords for attackers. Background images also improved password memorability.

1.1 Introduction to Draw-A-Secret
Jermyn, et al. [2] proposed a technique, called "Draw - a - secret (DAS)", which allows the user to draw their unique password (figure 1). In this technique user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated.

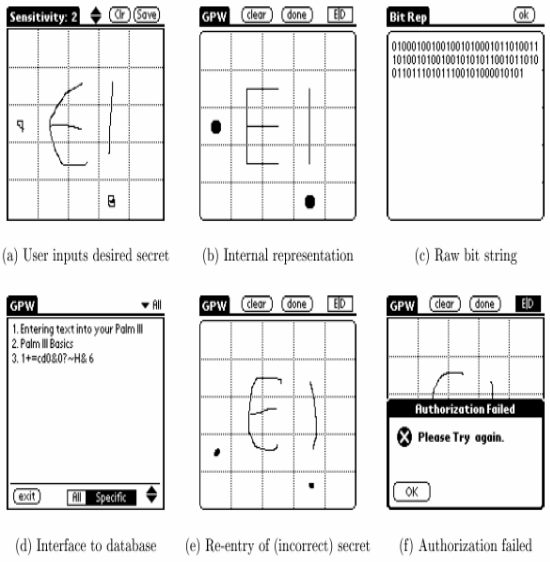


Figure 1 An example of DAS

There was some terminology used in the DAS which as Follows

First Term is known as the, stroke which is a Sequence Of cells crossing bounded at the both ends by PEN-UP Events [5].

As in the DAS scheme password is a sequence of strokes, so the length of password is the sum of strokes covered to generate the passwords. A high number of strokes ad lengths of password show the strength of password generated by the DAS [3]. Even stroke count, password length matters the most among all the factors. But the increasing the stroke count is not only the way to improving the security of DAS passwords. A low stroke count can be compensated for by increasing the password length [6].

2-PROPOSED WORK
In the proposed work our main motive is that to introduce the background image with the DAS so that the memorably and security van be enhanced. In our work both a background images and the drawing grid can be used to provide cued recall. But the question arises that which image will be suitable for the background image, for this we studied the "hotspots" (areas of interest) [7]. In our work we categorized people in two categories that are technical and nontechnical group. After

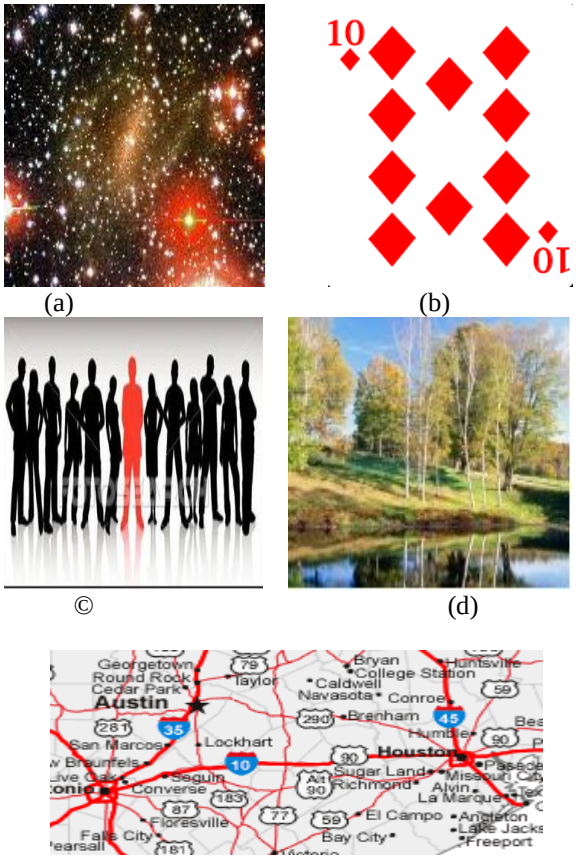
implementing the background image we analyze both the schemes with respect to different parameters.

3. PROCEDURE

For the purpose of our analysis we have taken a group of 10 People none of them had previously used DAS passwords. Participant backgrounds and occupations were also collected to see if the DAS scheme was as accessible to people from a technical background as those from a non-technical background. 6 persons were selected from the technical background and remaining selected from non technical background. Technical category included basically the students from engineering stream and non technical category included the staff members Like store in charge, shopkeepers in university who are not belonging from the technical background. In the first phase we invite these people for select the background image.

3.1. Back ground images used

In the following figure we showed the background images which we have used in our work. Their are various images taken from various categories keeping in mind of technical and non technical peoples. These images may be of space, nature, cards, crowd etc . We will discuss each and every image in detail which we have selected.



(a) (b) © (d) (e)

Figure 2 Background Images Used

The basic idea behind these images is that if a person selects image (a) then people can join dots to draw a secret, in image (b) people can draw a line through the design curve of cards. Same in the crowd images people in crowd can be joined each other to generate the draw a secret. In the route map persons can draw a secret by joining two cities by different routs. In our analysis technical people generally selected map and space pictures.

4. RESULTS

For our results we allowed 20 persons to generate their password both the techniques i.e. by DAS without background image and DAS with background image. we generate our results with parameters like time for generation and registration the passwords, stroke, password length and remembrance of passwords. These results are as follows.

4.1 Registration of passwords

The password registration in time shows the requirement of time for registration of password in login attempt the from both techniques. The table 1 shows that the mean time for generating the password in seconds. As we have taken the group of 10 people and analyze the time taken by them for registering the password from both techniques.

	1	2	3	4	5	6	7	8	9	10
DAS with Background image.	9.05	7.2	6.9	11.41	5.76	7.87	13.6	7.09	5.10	9.34
DAS Technique.	10.6	7.9	6.3	12.76	7.43	8.57	12.98	8.98	5.289	8.93

Table 1 Time taken by each user to generate the password by both techniques in seconds.

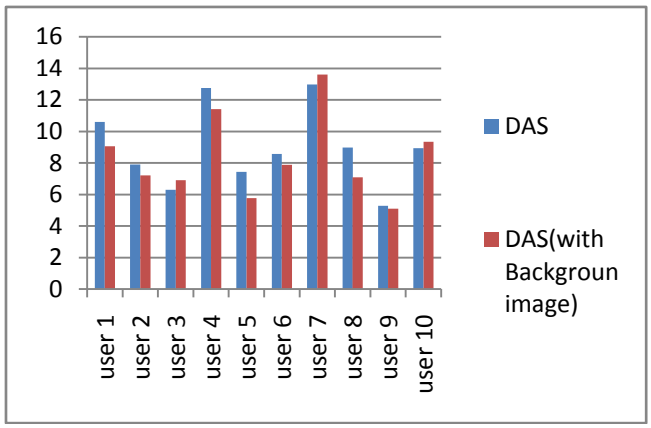


Figure 3: Graphical analysis of time taken to generate the password.

The above result shows about the registration time for every user in login. Result shows that 70% user took less time with help of background image in DAS.

4.2 Incorrect submission of passwords

In this analysis we gave five chances to every user to perform the action and then analyze that how many time users submit their passwords correctly. The results are shown as below.

	1	2	3	4	5
DAS using Background images	9	9	7	7	7
DAS	7	6	3	1	1

Table 2. Number of participants making incorrect password submission in the login phase

From the result we analyzed that in the first attempt 9 users with background image login their password correctly, but 7 users from simple DAS. In the second attempt the ratio rate increases. This difference increases with respect to attempts.

4.3 Recalling of passwords

In this section users are allowed to login their password after five minutes of registration and then after one week of registration. The results are as follows.

4.3.1 Recall Results after 5 minutes (Study 1)

When users are asked to login their password after 5 minutes time with both of technique the results are as follows.

Group	Response	Correct Response	%
DAS With Image	10	10	100%
DAS	10	9	90%

Table 3 Recall test (5 minutes Time Study-1)

4.3.2 Recall Results after 15 days time (Study 2)

When users are asked to login their password after 15days time with both of technique the results are as follows.

Group	Response	Correct Response	%
DAS With Image	9	7	77%
DAS	7	4	57%

Table 4 Recall Test (15 days Time Study-2)

We can see the result that after 5 minutes users using background image gave 100% response and users using only DAS gave 90 % response. Same in the case of 15 days response percentage is 77 and 57% respectively.

4.3 Security of Passwords

The password security can be defined as the minimum type of attack can break the passwords. In our analysis we have taken the four type of security attacks brute force attack, dictionary attacks, guessing and shoulder surfing. We identify these possible attacks on both the techniques and find the following result in terms of percentage.

Attacks	DAS	DAS With Background Image
Brute force attack	62.73	56
Dictionary Attacks	55.79	49.73
Guessing	19.56	16.10
Shoulder Surfing	23.25	22.91

Table 5 Types of attacks on techniques and their effect in percentage

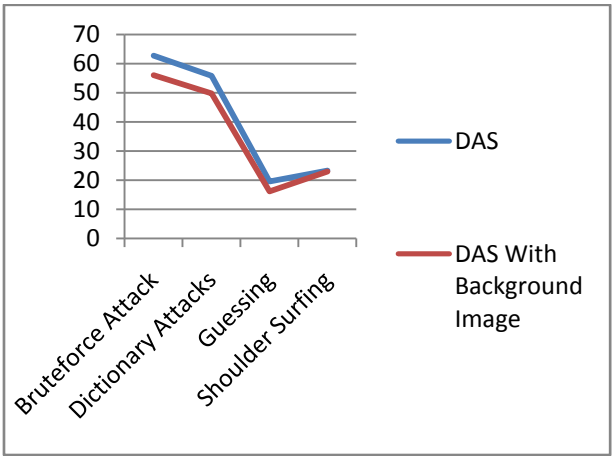


Figure 4 Possible attacks on both techniques in percentage.

5. SOFTWARE REQUIRED

For our analysis purpose we simulate our results in Mat lab. Results after making the DAS and DAS with background images are as follows.

(a)

(b)

Figure 5 Grid Selection using Background image (a) and without Background image (b)

6. CONCLUSION

This paper presents the analysis of Draw-a –Secret technique for graphical passwords and Draw-a- Secret with background image. Bothe technique are useful to generate a graphical passwords above results shows that in terms of password character sticks the DAS With background Image approaches are useful as it is less time taking also easy to remember. Also, this technique is easy to recall due to introducing of background images. Results show that the security level of such technique is better.

7. REFERENCES

[1] Graphical Passwords: A Survey Xiaoyuan Suo Ying Zhu G. Scott. Owen *Department of Computer Science Georgia State University.*

[2] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin. The Design and Analysis of Graphical Passwords, Proc. USENIX Security Symposium, 1999

[3] J. Yan, A. Blackwell, R. Anderson and A. Grant. Password Memorability and Security: Empirical Results. IEEE Security & Privacy, Vol. 2 No. 5, 2004.

[4] J. Yan. A Note on Proactive Password Checking. ACM New Security Paradigms Workshop, New Mexico, USA, 2001.

[5] J.Thorpe and P.C. van Oorschot. Towards secure design choices for implementation graphical password, ACSAC.2004, An extended version available at http://www.scs.carleton.ca/ jthrope/extendedStokes.pdf

[6] J. Thorpe and P. C. van Oorschot. Graphical Dictionaries and the Memorable Space of Graphical Passwords. Proc. USENIX Security Symposium, 2004.

[7] S Wiedenbeck, J Waters, JC Birget, A Brodskiy and N Memon. Authentication using graphical passwords: effects of tolerance and image choice. SOUPS'05, CMU, USA. ACM Press.

[8] The grafical login solution for your pocket pc – viskey http://www.sfrsoftware.de/cms/EN/pocketpc/viskey/index.html.