SG-PASS: A Safe Graphical Password Scheme to Resist Shoulder Surfing and Spyware Attack

Suryakanta Panda(✉) and Samrat Mondal(✉)

Department of Computer Science and Engineering,
Indian Institute of Technology Patna, Patna, India
{suryakanta.pcs15,samrat}@iitp.ac.in

Abstract. In general, it is difficult to remember a strong password i.e. a long and random password. So, the common tendency of a user is to select a weak alphanumeric password that is easy to remember. But the password which is easy to remember is also easy to predict. In contrast, the password that is very difficult to predict or requires more computation to break is also difficult to remember. To overcome this limitation of creating secure and memorable passwords, researchers have developed graphical password scheme which takes images as passwords rather than alphanumeric characters. But graphical password schemes are vulnerable to shoulder-surfing attack where an attacker can capture a password by direct observation. In this paper a graphical password scheme, namely SG-PASS is proposed which can prevent the shoulder-surfing attack by a human observer and also spyware attack, using a challenge response method.

Keywords: Graphical passwords · User authentication · Password security

1 Introduction

Authentication is an essential security component for many internet applications. It is a must for every system that provides secure access to confidential information and services. All the authentication techniques rely on at least one of the following methods:

- *Something you have:* it is also called as token based authentication. In this mechanism, each user has some physical identification objects which identify the user uniquely e.g. smart cards.
- *Something you know:* it is also called as knowledge based authentication. In this mechanism, a user has to remember an alphanumeric password or images for a graphical password.
- *Something you are:* it is also called as biometric based authentication. This includes the mechanism of fingerprint scan, iris scan etc.

A. Basu et al. (Eds.): IHCI 2016, LNCS 10127, pp. 27–38, 2017.
DOI: 10.1007/978-3-319-52503-7_3

Most systems use knowledge based authentication mechanism as it balances the usability, deployability and security issues. But the "password problem" [14] associated with alphanumeric passwords are expected to comply with two basic conflicting requirements-one is associated with usability and the other is related to security aspects.

1. *Usability aspects:* passwords should be easy to remember.
2. *Security aspects:* passwords should be secure, should be hard to guess; they should be changed frequently, and should not be same for any two accounts of the same user; they should not be written down or stored in plain text.

Meeting both of these requirements is the main challenge here. For this reason, users tend to choose and handle alphanumeric passwords very insecurely. Research has shown that when users fail to recall a password, they are often able to recall some parts of it correctly. But partially correct password cannot authenticate a user, only exact recall of complete password is required.

Various cognitive and psychological studies [10,12] indicate that pictures are much easier to remember than texts. This is the main objective behind graphical passwords which use images or shapes as a replacement for text. In a conventional graphical password scheme, a user selects several images as his/her password. During login the user has to click on the password images from a larger set of distractor images. If the user identifies the password images, that were selected in the registration phase and clicks on them, he/she is successfully authenticated [15].

However, clicking on images on a large, vertical screen may allow an observer to capture the password images. To address the above issue we propose a graphical password system which is resistant to the above said attack and is also resistant to spyware attack.

2 Related Work

Based on the authentication style, graphical password system can be broadly classified into three categories:

1. *Graphical passwords based on recognition:* In recognition based graphical password techniques, a user is asked to identify some images that he has selected during registration i.e. passface [4].
2. *Graphical passwords based on cued recall:* In cued recall based graphical password techniques, a user is asked to reproduce something that he has selected during registration phase i.e. passpoint [14], story [5].
3. *Graphical passwords based on pure recall:* In pure recall based graphical password techniques, a user is asked to redraw something that he has created during registration phase i.e. DAS [9], PassShapes [13].

Here we focus on graphical passwords based on recognition and based on cued recall rather than the password system based on pure recall.

A general approach to design a graphical password system is a challenge-response process. In this challenge-response process a user creates his/her password by selecting several images from a set of images. During the authentication phase, a challenge is thrown to the user by displaying some decoy image with a password image. In response, user has to successfully respond by identifying and clicking on the password image shown on the screen.

The first graphical password scheme proposed by Blonder [3], in which the user is asked to click on the approximate predetermined locations of a predecided graphical image in a correct order. The image can help users to recall their passwords and it is a better one as compared to recall alphanumerical passwords. However, the predetermined regions can be easily identifiable.

"Passpoint" system proposed by Wiedenbeck et al. [14] extended Blonder's approach by addressing some of its limitations. It allows arbitrary images instead of the predefined one and users can click on any place on the image to create their passwords. Here, the possible password space is quite large. However, there are some apparent points on the image which are usually chosen by users as their passwords. It makes the work easy for an attacker.

Based on the idea of passpoints, Suo [11] proposed a shoulder-surfing resistant password scheme in which the image is blurred except for a small focused area. Users can enter Y(for yes) and N(for no) to indicate that their click-point is within the focused area. If the click-points are a few, attackers can easily guess [7].

Based on the fact that humans can recall faces easier than other images Brostoff et al. proposed "passface" [4]. Here, users need to recognize and click on the face images that are selected in the registration phase. This procedure is repeated for several rounds. If the user correctly responds to each round, then he/she is successfully authenticated.

Similar to passface, Dhamija et al. [6] proposed a graphical authentication scheme which uses abstract images and concrete photographs instead of faces. For authentication, user is required to click on the password images from a set of decoy images and password images.

By utilizing the properties of convex hull, Sobrado et al. [15] proposed a protocol in which the system will show a number of graphical icons. For authentication, user identifies the pass icons, and then mentally forms a convex hull of the pass icons and clicks on a random point inside the convex hull.

Based on two protocols DAS [9] and Story [5], Gao et al. [8] proposed a new user friendly shoulder-surfing resistant scheme, called CDS. Here in password creation process a user selects several images as passwords and remembers them with their order of selection. During login, the user has to draw a curve across the password images orderly without lifting the stylus. However, its small theoretical password space and hotspots issue make it vulnerable to brute force attack and dictionary attack [7].

Combining text with graphic, Zheng et al. [16] proposed a hybrid password authentication scheme which uses shapes of strokes on the grid as the origin passwords and allows the users to login through text passwords. The basic idea

of this is to think some personal shape, map from this shape to text with strokes of the shape and a grid with text.

PassShapes [13] proposed by Weiss et al., authenticate users to a computing system by drawing simple geometric shapes constructed of an arbitrary combination of eight different strokes.

3 SG-PASS System

Our proposed scheme is a challenge-response mechanism and it uses approximately hundreds of graphical icons or arbitrary images shown in a window on the screen. In a challenge a user must identifies his or her password icons out of hundreds of displayed icons. Instead of direct input, the user responds to the challenge by entering keys from the keyboard keeping in mind that the shape formed by password icons on the screen matches with the shape of the entered keys of the keyboard. Two or three challenges are presented in sequence and if the user successfully responds to each challenge by entering the correct shape from the keyboard, then he or she is authenticated. It is based on recognition, an easier memory task than recall and users may create a story for sequence retrieval. In the following sections we describe the design and implementation in more detail.

3.1 Registration Phase

Our system uses a large set of images that are partitioned into different types for example, the images of sceneries, flowers, animals etc. A user can also add images of his/her choice. In registration phase, system will display a window consisting of approximately hundreds of images for creation of password. If a user feels uncomfortable with the images provided by the system, he/she can change that image window of his/her choice by adding different types of image. To create a password, the user chooses several images or icons from the window and also takes care about the order of selection of password images. Because, here the order of password images plays a vital role in authentication phase. The user has to remember the password images and their order that are selected by him/her. By creating a story a user may remember the order of password images.

3.2 Authentication Phase

In authentication phase, the password window containing same set of images but randomly permuted, is displayed to the user. These images include both password images and decoy images. User has to recognize the pre-selected password images and mentally draws a geometrical shape by connecting the password images in their respective order. Then the user enters keys anywhere from the keyboard [1] keeping in mind that the entered keys reflect the geometrical shape

(a) image 1 (b) image 2 (c) image 3

Fig. 1. Password images in their order

formed by password images displayed on the screen. This process of challenge-response is repeated more than once and the exact number depends on the system administrator. When the user has responded to a challenge (either correctly or incorrectly), another challenge comes, and this process continues until all challenges have been completed. The images are arranged randomly inside the window each time it is displayed on the screen, so the password images move to new positions. A brief outline of the authentication steps for the proposed SG-PASS scheme is given below.

Authentication Steps

1. Identify all the password images from the set of images shown in the window screen. Now their relative positions are located.
2. Map the bottom most password image to the lowest row of the keyboard.
3. Find the row difference between top most password image and bottom most password image.
4. Keeping in mind, the total number of rows in password window to the total number of rows in keyboard (only four), map the topmost password image to the keyboard.
5. Then map the rest password image, accordingly.
6. After the process of mapping, enter the keys as per the order of preselected password images, such that the entered keys reflect an approximate shape formed by password images.

3.3 Discussion

Figure 2 shows a password window which has the password images of Fig. 1 and some decoy images (here we are considering only the faces of celebrities, user can also change the window so that one window may contain different types of images i.e. scenery, flowers, animals etc.). User can identify the password images and try to map the shape by entering the keyboard characters like “TCB” or “EZC” or “YVN” as “TCB”, “EZC” are reflecting an approximate shape formed by the password images. But the system cannot accept “TVN” as password because it is not reflecting the shape formed by password images (Figs. 3, 4 and 5).

Fig. 2. Window1

Fig. 3. TCB, a valid response

In the prototype we have taken only three images as password images. One can take more than that also but the minimum number is three. During authentication only three images are considered at a time. Assume that, one user has selected four images as password image i.e. image1, image2, image3, image4. In authentication, the user will consider the first three images, that is, image1, image2, image3 and selects three keys from the keyboard accordingly. After that, in the same round, the user will take the next three images that is, image2, image3, image4 and selects three keys as per image2, image3, image4. Thus, the user will have to enter six keys at a time for password size of four.

Fig. 4. EZC, a valid response

Fig. 5. TVN is not a valid response

4 Security and Usability Analysis

In this section, different security and usability factors of SG-PASS scheme is analyzed.

4.1 Mouse-Loggers

Mouse-loggers are used to record the click position and trajectory of the mouse. It can crack the password schemes which use mouse for input information [7]. Mouse-loggers are not a threat to our proposed scheme as we are giving information to the system using the keyboard not using mouse.

4.2 Keystroke-Loggers

The main idea of our proposed scheme is making a shape based password using the images and text input. The text characters that user will input are different in different login session. This mechanism can prevent key-logger attack. If an attacker records the input characters then he would get nothing about the password images.

4.3 Accidental Login

Assume that the number of password image is three and only two round of challenge response is there. Using three password images many different shapes are possible. If we consider only ten distinct shapes like in Fig. 6, then the probability of successful accidental login can be computed as below.

As we are considering the order, for each image six different orders are there (we are taking three password images in the prototype, it gives $3! = 6$ different types of permutation). So, using three password images there are 60 different passwords. For two round of challenge-response, the probability of successful accidental login becomes $(1/60)*(1/60) = 0.00028$ which is quite low.

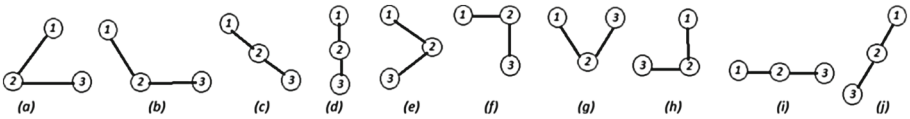

Fig. 6. Some possible shapes formed using three password images

4.4 Shoulder-Surfing Attack

The login process does not reflect the password images directly. Attacker can get the shape formed by password images by observing the text characters entered by the user. But, that shape cannot reveal the password images because for a single geometrical shape there are many combinations of password image. Consider the password window in Fig. 2, here many corresponding shapes can be formed by characters "TCB", some are given in Fig. 7.

Fig. 7. Corresponding shape for characters "TCB"

In addition as the password images changing their positions randomly inside the password window, a human observer cannot remember exact positions of all the images in a particular window.

4.5 Brute Force Search

The general mechanism to defend brute-force search is to increase the password space. Assuming that there are hundreds of images in a password window, the password space can be calculated as C(100,3) = 161700

However, it is difficult to carry out brute-force search in graphical passwords compared to alphanumeric passwords because computers spend considerable amount of time for identifying the password images in a password window.

4.6 Phishing

Phishing is a difficult one for graphical password scheme as compared to alphanumeric passwords. In the alphanumeric password scheme attackers need not require to know anything about user's password or theory behind authentication process. The fake website will record user name and password as entered by user. However, in graphical password system the attacker must know how the authentication process works and it is different for different graphical password scheme. In our scheme, the password window is different for different users as one can add images of his/her choice and users are not giving direct input for passwords. So, it is a difficult task for attackers to get passwords through phishing.

4.7 Usability Analysis

Fifteen participants including university students and non-technical staff took part in the evaluation process of SG-PASS scheme. After training, they took 27.6 s on average for each round of SG-PASS and found that it is easy to remember and a simple one. For the target of ten correct login, five participants accomplished in first ten attempts. However, the remaining participants reach the target with one to three extra attempts. The details are given in Table 1. The percentage of successful login attempts out of total login attempts by all users is found to 89 percent.

5 Comparison with Other Recognition Based Graphical Systems

In Sect. 2, we discussed various graphical password systems that use the recognition technique for authentication. We compare our system, SG-PASS with these password systems in terms of security and usability strength.

From Table 2, we can conclude that only two schemes CHC [15] and Zheng [16] can prevent both spy-ware and shoulder-surfing attacks. However, the distribution of response points are not uniform (more concentrated at center) in CHC, which makes the attacker's work easy. In Zheng et al.'s methodology [16], users have to remember exact locations of the grid cells like DAS, which puts an extra memory burden. In a nutshell, the comparative results are presented in Table 2. It shows SG-PASS has relatively higher security and usability features

Table 1. Details of usability analysis

Users	Avg. login time in sec	Unsuccessful attempt
User1	30	2
User2	25	3
User3	23	0
User4	22.4	0
User5	25	2
User6	26.1	1
User7	27	0
User8	27.3	1
User9	30	2
User10	28.2	0
User11	33.5	2
User12	29	0
User13	35	2
User14	25.3	1
User15	27	2

Table 2. Comparison with other methodology

Schemes	Spy-ware resistant	Shoulder-surfing resistant	Comment
Blonder [3]	N	N	Number of predefined regions are small and easily identifiable
Passpoint [14]	N	N	Care must be taken to eliminate hot spots
Suo [11]	N	N	Attackers can easily guess if few click-points are used
Passface [4]	N	N	Face images are clearly visible
Dhamija [6]	N	N	A recondite picture is hard to remember
CHC [15]	Y	Y	Distribution of the response points are not uniform [2]
CDS [8]	N	Y	Password space is very less
Zheng [16]	Y	Y	Users have to remember exact locations of the grid cells like DAS [9]
SG-PASS	Y	Y	Simple, easy to remember and resist all the attacks discussed in Sect. 4

compared to existing graphical password schemes. However, like other schemes it also suffers from intersection issue. An intersection attack is possible when the attacker is able to record the password window and the keys for multiple sessions.

6 Conclusion and Future Work

The contribution of this paper is the design of a graphical password scheme that extends the challenge-response model to resist spy-ware and shoulder-surfing attacks. Users can create a valid graphical password easily and quickly but face some difficulty in learning their passwords. This scheme is easy to execute and more secure and usable as compared to other graphical password approaches. It provides a simple and intuitive technique for users to authenticate. However, like other graphical password system, the issues in this system is the intersection analysis. To overcome this issue, we plan to design a more advanced system without compromising the security and usability aspects.

References

1. Ameer, D., Al-Absi, A.A., Mohammed, A.O., Habbal, A.M.M., Hassan, S.: Anywhere on-keyboard password technique. In: 2010 IEEE Student Conference on Research and Development (SCOReD), pp. 159–163. IEEE (2010)
2. Asghar, H.J., Li, S., Pieprzyk, J., Wang, H.: Cryptanalysis of the convex hull click human identification protocol. Int. J. Inf. Secur. **12**(2), 83–96 (2013)
3. Blonder, G.E.: Graphical password, uS Patent 5,559,961, 24., September 1996
4. Brostoff, S., Sasse, M.A.: Are passfaces more usable than passwords? a field trial investigation. In: People and Computers XIV Usability or Else!, pp. 405–424. Springer (2000)
5. Davis, D., Monrose, F., Reiter, M.K.: On user choice in graphical password schemes. In: USENIX Security Symposium, vol. 13, p. 11 (2004)
6. Dhamija, R., Perrig, A.: Deja vu-a user study: using images for authentication. In: USENIX Security Symposium, vol. 9, p. 4 (2000)
7. Gao, H., Jia, W., Ye, F., Ma, L.: A survey on the use of graphical passwords in security. J. Softw. **8**(7), 1678–1698 (2013)
8. Gao, H., Ren, Z., Chang, X., Liu, X., Aickelin, U.: A new graphical password scheme resistant to shoulder-surfing. In: 2010 International Conference on Cyberworlds (CW), pp. 194–199. IEEE (2010)
9. Jermyn, I., Mayer, A.J., Monrose, F., Reiter, M.K., Rubin, A.D., et al.: The design and analysis of graphical passwords. In: Usenix Security (1999)
10. Shepard, R.N.: Recognition memory for words, sentences, and pictures. J. Verbal Learn. Verbal Behav. **6**(1), 156–163 (1967)
11. Suo, X.: A design and analysis of graphical password (2006)
12. Suo, X., Zhu, Y., Owen, G.S.: Graphical passwords: a survey. In: 21st Annual Computer Security Applications Conference (ACSAC'05), pp. 463–472. IEEE (2005)
13. Weiss, R., De Luca, A.: Passshapes: utilizing stroke based authentication to increase password memorability. In: Proceedings of the 5th Nordic Conference on Human-Computer Interaction: Building Bridges, pp. 383–392. ACM (2008)

14. Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., Memon, N.: Passpoints: design and longitudinal evaluation of a graphical password system. Int. J. Hum Comput Stud. **63**(1), 102–127 (2005)
15. Wiedenbeck, S., Waters, J., Sobrado, L., Birget, J.C.: Design and evaluation of a shoulder-surfing resistant graphical password scheme. In: Proceedings of the working conference on Advanced visual interfaces, pp. 177–184. ACM (2006)
16. Zheng, Z., Liu, X., Yin, L., Liu, Z.: A hybrid password authentication scheme based on shape and text. J. Comput. **5**(5), 765–772 (2010)