International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 16 (2017) pp. 6091-6096

Shoulder-Surfing Resistant Graphical Password System for Cloud

Vijayakumari Rodda[1], Gangadhar Rao Kancherla[2] and Basaveswara Rao Bobba[3]

[1]Assistant Professor, Department of Computer Science, Krishna University, Rajupet, Machilipatnam, Andhra Pradesh, India.
Orcid Id: 0000-0002-6695-8807

[2]Assistant Professor, Department of Computer Science and Engineering, Acharya Nagarjuna University, Nagarjuna Nagar, Guntur, Andhra Pradesh, India.

[3]Systems Programmer, Department of Computer Science and Engineering, Acharya Nagarjuna University, Nagarjuna Nagar, Guntur, Andhra Pradesh, India.

Abstract

Cloud based applications authenticate users before they are allowed to access the services provided by them. Most commonly used user authentication mechanism is text-based password systems. Graphical passwords have been proposed because the pictorial-superiority effect suggests that people have better memory for images. After a comprehensive study on various graphical password schemes, it is found that they suffer from vulnerabilities of shoulder surfing attack and teasing the user by using several steps during login. The main objective of this research is to implement a secure shoulder-surfing resistant authentication scheme by providing the variable size grid to select images during login phase. For resistance, two ways of inputting the password is possible with this scheme. In order to analyze security, a shoulder surfing attacking session was conducted in the university with questionnaire utilized the user's feedback on security of proposed scheme. The results show that the proposed scheme can effectively balance the two symbiotic pillars of usability and security by increasing resistant to shoulder-surfing attack.

Keywords: graphical password, authentication, shoulder-surfing, usability, security

INTRODUCTION

Text based passwords are the most widely used for authentication. But this traditional technique has its own flaws and is vulnerable to attacks. One of them is the shoulder surfing attack that can be performed by an antagonist to obtain user's password by watching over the user's shoulder as he enters his password. Traditionally, shoulder surfing attacks also called "peeping attacks" concerns moved from telephone calling card fraud to automated teller machine (ATM) fraud, and more recently to mobile computer users. Most graphical authentication systems are based on either recognition based or recall based [1]. In recognition-based systems a user must recognize images chosen during registration phase from a large group of decoy images. There can be only two possibilities that the image is recognized or unknown [2]. In recall-based password systems users must click on several areas chosen at the time of registration in an image, cued by viewing the image. It is known that recognition memory is better than unaided recall [3].

Furthermore, psychological studies show that images are recognized with very high accuracy (up to 98 per cent) after a two hour delay, which is much higher that accuracy for words and sentences [4]. Hence, we propose a scheme to improve a recognition based scheme (Passface) which not only reduce the threat of shoulder-surfing but also has an added benefit of expeditious recognition and usability, thus reducing some flaws of recognition based systems.

The paper discusses related work in the field of password authentication followed by the description of proposed scheme. Later, the usability and security study is presented. The conclusion and future work concludes the paper.

RELATED WORK

Graphical Password Authentication Schemes are classified as recall-based password schemes and recognition-based password schemes. In recall-based schemes, a user is requested to recreate something that he or she made at the time of registration. In recognition-based schemes, a user is given an arrangement of pictures and the user gets validates by perceiving and distinguishing the pictures, he or she chooses at the time of enrolment.

Recall Based Graphical Password Schemes

Recreating a drawing and replacing a selection are the fundamental sorts of recall-based systems. Replicate a drawing strategy incorporates Draw-a-secret(DAS), Passdoodle System, Syukri Strategy, and so forth. Jermyn et

al. [5] proposed DAS method, which permits user to draw their remarkable password. A user is demanded to outline a photo on the 2D grid and the drawing's coordinates are saved in a succession. For authentication, the user has to re-draw the picture with the same coordinates in a specified order. Passdoodle method developed by Goldberg et al. [6] contains handwritten outlines generally drawn with a stylus on a touch screen. Syukri et al. [7] proposed a framework where verification is led by having user drawing their signature utilizing mouse. The system can modify the signature area and by enlarging or scale-down signatures and also by rotating if needed. The database stores this data and first takes the client information along with the signature's parameters for verification utilizing geometric normal means subsequent to performing the normalization once more.

In repeat a sequence of sections group of authentication algorithms, a user is solicited to rehash arrangements from activities at first done by the user at the registration process. Strategies having a place with this classification incorporate Blonder System, Passpoint strategy, Passlogix technique, and so on. Blonder [8] developed a graphical password scheme in which a password is created by user tapping on different areas of a picture. During confirmation, the user must tap on the estimated territories of those areas. Passpoint method proposed by Wiedenbecl et al. [9] that had developed Blonder's thought by evacuating the predefined limits and allowing distinctive arbitrary pictures to be utilised. Along these lines a user can now tap on any point of a picture for makeing a password and after that resilience about each chose pixel is ascertained. Keeping in mind the end goal to be authenticated, the user ought to click anyplace on the picture within the tolerance of the pixels that are chosen and also in a correct sequence. Passlogix method [10] has the bases of Blonder idea. For validation, the users must tap on diverse things of the picture in the predefined grouping. Boundaries are characterized for everything undetectably so as to check if an item is chosen by mouse. Other related works can be found in [11]. MK Rao et al. [12] proposed a graphical password scheme for cloud services which combines recall based and recognition based techniques. First, user has to produce an age sequence in recall phase and later, at every selected age the registered image must also be identified in recognition phase. This scheme also provides the recovery system for the password, but it burdens the user by making him remember too many things for password. Karmajit Patra et al [13] presented implementation of cued click point graphical password which uses circular tolerance. This scheme was basically based on the nature of click point on the image and circular tolerance. The image and click point are one to one relation in nature till (n-2)th click point where n is the password length. In this, a password length of four uses three images. Mrs.Gokhale et al [14] introduced a graphical password technique which has two phases called registration and login. During registration, the user has to select some even number of images to set as a password. Later any other picture can be selected by the user to select any three questions. The answers to the questions must be any three regions on the later selected image. User has to click on region of answers and save them for login purpose along with his other details. During login, the user has to select the appropriate images and also answer the questions correctly. Amol Bhand et al [15] proposed a click based recognizable graphical password authentication system. In this system, at the time of registration user gets one system generated text password on his e-mail on the basis of RGB values of the selected click points of the image. While logging in user has to enter this text password.

Recognition Based Graphical Password Schemes

Dhamija et al. [16] proposed a graphical password scheme in which the client is given an arrangement of irregular pictures. From these pictures the client chooses a succession of pictures and for validation the client is told to recognize the pre-chosen pictures. Sobrado and Birget [1] built up a shoulder surfing resistant graphical password scheme that showcase a blend of pass-articles (pre-chosen by client) and numerous difficult items. The scheme instructs the client to snap inside the convex hull space surrounded by all the pass-objects for verification.

In Man et al. [17] user chooses several pass-objects and the algorithm provides each of the pass-object with diverse variants and distinctive code. For verification, the client is given a few scenes where every scene contains a few pass objects long with some fake objects. The client needs to type in a string with the codes of the individual pass-object variations distinguished in the scene. Jansen et al. [18] thesis has led to create an authentication scheme for mobile devices. During registration phase, a client chooses a topic (e.g. ocean, house and so forth) that contains thumbnail photographs and afterward indicates a grouping of pictures in a sequence. Takada and Koike [19] likewise recommended a comparative graphical password scheme for mobile devices that has a few phases of check for verification. This technique permits users for the usage of their favourite image to get authenticated. The clients first register their most loved pictures (pass-pictures) with the server. At every round, the client either might indicate a pass-picture among a few bait pictures or choose nothing if there is any pass-picture present. Real User Corporation submitted Passface Algorithm [20] in which the client needs to indicate four pictures of human appearances from an information base that contain faces for their future password. In the verification stage, the system displays a grid of nine confronts, a mix of one face already picked by the client and eight distraction faces. A shoulder-surfing resistant graphical password authentication mechanism was proposed by MK Rao et al [21]. In this mechanism, user password is processed as pass-characters one pair at a time sliding to the

right one character at a time, wrapping around until the last pass-character forms the first element in the pair. Once the pass characters are identified each pair is processed separately using predefined rules. Amish shah et al [22] proposed shoulder-surfing resistant graphical password system to minimize the search time to find the pass-images on a login screen. This scheme uses texts in images instead of objects such that quicker recognition can take place. Each and every image has two characters in it. The user can select an alpha numeric pass phrase at the time of registration. During login, the user will have to move the frames with appropriate characters and arrange them as per the alignment chosen during registration. Abutalha et al [23] proposed an alignment based graphical password scheme. It has two phases: select, training phase and identification phase. In first phase, user has to register username and password pictures. He is also trained to remember images in this phase. In the second phase, user has to identify and align the pass pictures displayed in circles. The number of circles displayed is equal to number of password pictures selected. Each and every circle consists only one pass picture during login. So, he has to align them and submit them to get access to the system. K. Gangadhara Rao et al [25] proposed a click based graphical password authentication system. There are two phases – registration and login. The user has to register by giving his username and password and the selected password is shifted circularly to the right by one character and stored in the database. Login procedure happens in four sages and in each stage the entered input is compared with the rotated, stored, password string by shifting one character to the left by 'n' number of times. Here 'n' represents the number of iteration. If all the four stages are successfully passed by the user, then he is allowed to access the system.

PROPOSED METHOD

In this section we will consider a shoulder surfing resistant graphical password scheme based on Passface Scheme [24]. The Passface scheme given by Real User Corporation is a recognition-based graphical password authentication scheme. This scheme is enhanced in the proposed scheme to provide more usability and security. There are two phases in the proposed scheme. Registration Phase and Login Phase. During registration the user provided with an interface which has a provision for entering username and a bunch of images to select his/her pass image. The images are displayed in a 5x5 grid for the user to select from as shown below:

Figure 1. Registration Screen Example [Source: Krishna University Website]

The user can select the pass images either from the shown images or he also can ask the server to provide still more images to select from. The user has to select totally four images as his pass images. When the user asks for more images the existing 5x5 grid is replaced with the new pictures brought from the server. The database can store upto 1200 images.

During login the user is asked to enter his/her user name and the size of the grid to display images to select pass images from. The interface at the time of login will be as shown below:

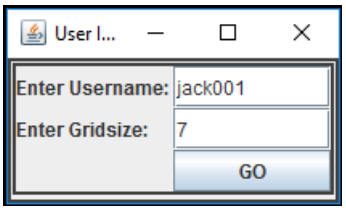

Figure 2. Example of Login Screen to enter user name and grid size

After selecting the grid size the user is provided with an interface which displays a pass image along with decoy images. The user has o select the pass image either by clicking on the image by mouse or by entering the position of the image (row number, column number) in the grid as shown below:

Figure 3: Login Screen to select images [Source: Krishna University Website]

After selecting the pass image the user has to click on the button "next" such that the user is directed to next set of images to select the next pass image. This process repeats for four times as he/she has to select four pass images. After selecting the fourth image correctly, the user is allowed to get access to the cloud applications.

Implementation

The proposed scheme was implemented using java. The database used was MySQL. Development tool used for application building was eclipse.

Software Requirements:

Technology Used: Java

Database: MySQL

Development Tool: Eclipse/Net Beans

Hardware Requirements:

PC/Laptop

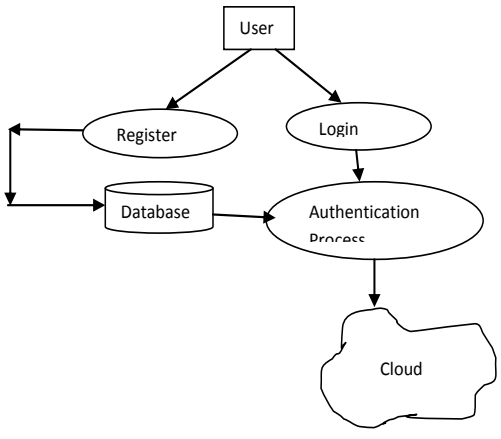

Figure 4. Implementation of proposed scheme

RESULTS AND ANALYSIS

Password Space

In the proposed scheme, a user has to select four images as his password. The data base contains 1200 images. Therefore, total number of possible passwords is $1200C_4$. Hence, the password space for the proposed scheme is 8.596×10^{10} approximately.

Usability and Security

A user study was conducted by involving 20 Post Graduate Students studying in the university Computer Centre to study usability and security features after a learning session on the proposed scheme. Students are divided into two groups, ten members in each group. First group of students were given systems to register their usernames and passwords. The first group students are called users while the second group of students are called observers. Each and every observer is attached to a unique user. The registered users are asked to login to the systems using the proposed scheme. First five of the users are asked to use mouse for login procedure and the other five are asked to use keyboard to login. The observers were allowed to observe the login procedure of the users from two feet distance. This login and observation procedure was repeated for five times.

Then users are given Feedback form-1 to describe about the usability features of the proposed scheme. The observers are given Feedback form-2 which contains 100 images to find out the pass images of the user they observed. Feedback form-1 contains the following questionnaire:

1. Is it easy to create?
2. Is it easy to use
3. Is it easy to memorize?
4. Is it easy to execute?
5. Is it fast to execute?
6. Does it have pleasant interface?
7. Does it contain pleasant pictures?
8. Is it reliable?
9. Is it acceptable in real world?

Users are asked to write "YES" or "NO" to the above questions. The average acceptance (i.e., "YES") given to Feedback form-1 was 96.7

The second group i.e., the observers group are asked to select pass pictures of the user whom they observed. The observers report is shown below in Table-1.

Table 1. Observers Report

Observers	Success Rate						
	Trial-1	Trial-2	Trial-3	Trial-4	Trial-5	Total	In Percentage
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	1/4	1/4	1/4	25
7	1/4	1/4	1/4	2/4	2/4	2/4	50
8	0	0	1/4	1/4	1/4	1/4	25
9	0	1/4	1/4	1/4	1/4	1/4	25
10	0	0	0	0	0	1/4	25

From the observers report, it is known that first 5 observers among 10 were totally failed in identified password pictures in the shoulder surfing attack. The first five observers used keyboard to login to the system. Second five observers used mouse. Four of the observers those who used mouse succeeded 25%, where as only one observer succeeded up to 50%. But none of them succeeded 100%. i.e., none of the observers were able to capture the password in shoulder surfing attack. Consider the success percentage of second group of observers in Table-2. We can take the mean for the purpose of analysis.

Table 2. Report of observers those who used mouse for login

Observer	6	7	8	9	10
Success Rate	25	50	25	25	25

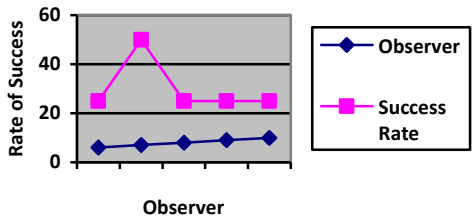

Figure 3. Mean of the success rate of observers those who used mouse for login

From the mean of the success rate of observers it is clear that, there are only 30% of chances in cracking the password by using mouse to login. Hence, the system is 70% secure when we use the mouse for login. Whereas when use keyboard to login to the system, the system is 100% secure.

Let 's' be the size of the grid used for displaying and inputting the password pictures. There will be 's×s' number of pictures displayed on the screen to select from, for logging in. Totally four pictures must be selected from 's×s' number of pictures. If the user is using keyboard for login procedure, then there is no problem. If the user uses mouse, then the complexity of the problem must be considered. If the size of the grid is small, then there is chance of succeeding in shoulder surfing attack. If the size of the grid is large, then the chances of succeeding in shoulder surfing attack may diminish.

CONCLUSION

A graphical password scheme is proposed to eliminate the shoulder surfing attack efficiently. So the login user's cloud services/applications are protected by using this system. Most studies on security and usability seem to confirm the belief that the system can be either secure or usable, but researchers try to build or enhance systems which balance both. This paper proposed a scheme for enhancement on usability and security of graphical password authentication. For increasing usability, it tries to cover most usability attributes based on ISO definitions of usability. In terms of security, the system tries to mitigate shoulder surfing attacks by providing variable size grid for selecting password during login. The results show that the new system is 100% resistant to shoulder surfing when we use keyboard to login, but only 70% secure when we use mouse to login. In case of usability it achieves 97% of usability.

There are also certain limitations in the proposed scheme. If the distance between the login system and observation point is reduced and the users use mouse to login, the rate of success in identifying the password pictures may improve. If the number of attempts to observe the password are increased, then also the success rate of capturing the password in shoulder surfing attack may increase. These limitations can be overcome in our future work.

REFERENCES

[1] Suo X, Zhu Y, Owen GS. Graphical passwords: A survey. In Computer security applications conference, 21st annual 2005 Dec 5 (pp. 10-pp). IEEE.

[2] Wiedenbeck S, Waters J, Birget JC, Brodskiy A, Memon N. Authentication using graphical passwords: Effects of tolerance and image choice. In Proceedings of the 2005 symposium on Usable privacy and security 2005 Jul 6 (pp. 1-12). ACM.

[3] Norman D. The design of everyday things: Revised and expanded edition. Basic Books (AZ); 2013 Nov 5.

[4] Shepard RN. Recognition memory for words, sentences, and pictures. Journal of verbal Learning and verbal

Behavior. 1967 Feb 1;6(1):156-63.

[5] Jermyn IH, Mayer A, Monrose F, Reiter MK, Rubin AD. The design and analysis of graphical passwords. USENIX Association.

[6] Goldberg J, Hagman J, Sazawal V. Doodling our way to better authentication. InCHI'02 extended abstracts on Human factors in computing systems 2002 Apr 20 (pp. 868-869). ACM.

[7] Syukri A, Okamoto E, Mambo M. A user identification system using signature written with mouse. InInformation Security and Privacy 1998 (pp. 403-414). Springer Berlin/Heidelberg.

[8] Chiasson S, van Oorschot PC, Biddle R. Graphical password authentication using cued click points. In ESORICS 2007 Sep 24 (Vol. 7, pp. 359-374).

[9] Wiedenbeck S, Waters J, Birget JC, Brodskiy A, Memon N. PassPoints: Design and longitudinal evaluation of a graphical password system. International journal of human-computer studies. 2005 Jul 31;63(1):102-27.

[10] Boroditsky M. Passlogix password schemes. http://www. passlogix. com. 2002.

[11] Biddle R, Chiasson S, Van Oorschot PC. Graphical passwords: Learning from the first twelve years. ACM Computing Surveys (CSUR). 2012 Aug 1;44(4):19.

[12] Rao MK, Switha TU, Naveen S. A Novel Graphical Password Authentication Mechanism for Cloud Services. In Information Systems Design and Intelligent Applications 2016 (pp. 447-453). Springer, New Delhi.

[13] Patra K, Nemade B, Mishra DP, Satapathy PP. Cued-Click Point Graphical Password Using Circular Tolerance to Increase Password Space and Persuasive Features. Procedia Computer Science. 2016 Jan 1;79:561-8.

[14] Gokhale MA, Waghmare VS. The shoulder surfing resistant graphical password authentication technique. Procedia Computer Science. 2016 Jan 1;79:490-8.

[15] Bhand A, Desale V, Shirke S, Shirke SP. Enhancement of password authentication system using graphical images. In Information Processing (ICIP), 2015 International Conference on 2015 Dec 16 (pp. 217-219). IEEE.

[16] Dhamija R, Perrig A. Deja Vu-A User Study: Using Images for Authentication. In USENIX Security Symposium 2000 Aug 14 (Vol. 9, pp. 4-4).

[17] Man S, Hong D, Matthews MM. A Shoulder-Surfing Resistant Graphical Password Scheme-WIW. In Security and Management 2003 Jun 23 (pp. 105-111).

[18] Jansen W. Authenticating mobile device users through image selection. WIT Transactions on Information and Communication Technologies. 2004 Apr 7;30.

[19] Takada T, Koike H. Awase-E: Image-based authentication for mobile phones using user's favorite images. Human-computer interaction with mobile devices and services. 2003:347-51.

[20] Authentication RU. The Science Behind Passfaces. White Paper, June. 2004.

[21] Rao MK, Pravallika CV, Priyanka G, Kumar M. A shoulder-surfing resistant graphical password authentication scheme. In Innovations in Computer Science and Engineering 2016 (pp. 105-112). Springer, Singapore.

[22] Shah A, Ved P, Deora A, Jaiswal A, D'silva M. Shoulder-surfing Resistant Graphical Password System. Procedia Computer Science. 2015 Jan 1;45:477-84.

[23] Danish A, Sharma L, Varshney H, Khan AM. Alignment based graphical password authentication system. In Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on 2016 Mar 16 (pp. 2950-2954). IEEE.

[24] Real User Corporation, Passfaces TM, www.realuser.com, Accessed on January'07

[25] Rao K.G., Vijayakumari R, Rao BB. 4-Stage Graphical Password Authentication Scheme for Cloud. Journal of Theoretical and Applied Information Technology. 2017. Jan 15:95(1). Pp. 105-114.