DASSA: RECOGNITION BASED GRAPHICAL PASSWORD

SWATI KUMARI AND RUHI OBEROI
Mgm's Jawaharlal Nehru Engg.college Aurangabad,Maharashtra,India
Email: swati2789@gmail.com

ABSTRACT: Recognition based Graphical password is secure against shoulder surfing attack, guessing and capture attacks. In this paper we propose a technique to defense against shoulder surfing attack. This technique is based on grid of images, where the user first give his username and then identifies the password images by mentally eliminating rows and columns that does not contain password images apply this process twice and then mapped the password into another blank grid.

KEYWORDS: authentication, graphical password, shoulder surfing attack ,NET, SQL, Windows.

INTRODUCTION

Graphical password uses the images instead of text, human being easily remember images than the text .In Recognition based graphical password (RBGP) user has to recognize the images from a set of images in the login session. RBGP has the features of memorability for example in passface technique the user will be asked to choose four images of human faces from a face of database as their future password in the authentication process the user can randomly clicks on the known faces and if it correctly identifies the four faces then the user is authenticated, this system shows that passfaces are very memorable .Another feature is usability the visual mode of interaction is easy and it does not depend on any language different types of people is comfortable of using it. Such an interaction is also ideally suited for hand-held devices and touch-based systems where the text entry is awkward or limited [1][2] .Another feature of RBGP is highly security than text based password it can resist our system from shoulder surfing attack, dictionary attack as [3]paper says this. it is also Reliable here the error rate is set carefully .Knowledge based authentication system fall into two categories one is text password and another is graphical password both the password is depend on the knowledge of individual for example alphanumeric characters entered by the user is password and it is assumed that only authenticated person can identify their password and hence ones identify gets verified. However in reality anyone who knows password can authenticate themselves as an authenticated person. Text password can be easily verified by another person as compared to the graphical password, because text password can be a person's name or his friends name or mobile number, in graphical password it is not easy to break the system several advantages are given above. Apart from several advantages RBGP is not widely used due to some problems like storage and communication graphical password required much storage space than the text password, thousands of pictures have to be maintained in a centralized database [4]. Memory management is one of the issues. Shoulder surfing attack is one such attack ,aimed at capturing passwords through direct observation while the legitimate user is entering the information during the authentication [3] example automated trailer machine in the ATM if user is entering his pin any person who is standing with him can observe the pin and may stolen his password. Another such attack is dictionary attack, in this attack the preset words are checked in dictionary for test whether they used as a password. One such main reason is Guessing Attack where the attacker wants to guess the users password by taking some of its personal information like his pet name, his name, his mobile number. RBGP are vulnerable to observation attack

because their mode of interaction is visual in nature and the complete password remains visual on the screen during the entire login session [3].

In this paper, we propose a technique for RBGP where user has to first enter his user name. Then it presents two grids. sA grid which contains images is longer and the blank grid is smaller so the mapping is not directly done. So in order to map the larger grid of images to smaller one user has to first eliminate that row and column which does not contain password images apply this process twice ,then map the password images into the smaller blank grid. For every session password position is changed. This technique widely resist against shoulder surfing attack ,Guessing attack ,observation attack and many more .Recognition based graphical password is basically more secure then the text based graphical password.

Rest of the paper organized into several parts: Motivation part, Literature survey, Graphical password security aspects, proposed system, Experimental result, Conclusion.

MOTIVATION

Knowledge based authentication mechanism typically text based password are well known [5]. Text based password has usability to smaller password which can be easily guessed because each time user enters the same password so anyone can easily guess the password if he/she carefully watched the login process so in order to reduce the guessability attack one effective solution is given utilize the one time password it is only valid for one session but it is not practically possible to create large number of password list for one time password and long text based password provides high security but hard to remember. knowledge based authentication mechanism has one more category graphical password, it has high usability because human brains easily recognize or remember images or pictures than text the success of graphical password is mostly depends on the type of image which we are using like personal image or random image. It provides high security because it is hard to guess and changed frequently order of imaged does not play an important role in RBGP so it is easy for user to remember the password. Graphical password is user centric control whenever one is actively involved in any cognitive activity or process an Action Event memory, stronger than the recognition memory is active[6]. RBGP provides high memorability, usability, good security [2].

Taking above guidelines, we are motivated to develop a shoulder surfing defense for RBGP which also provides security against guessability , observation attacks and it is easy for user to remember. Maintaining the Integrity of the Specifications.

LITERATURE SURVEY

Graphical password is a technique where password is in the form of images rather than text. As more user is familiar with text password and conventional textual password authentication schemes have no shoulder surfing resistance. Zhao[7],proposed a shoulder surfing resistance graphical password S3PAS,in which user has find the textual password and then mix the textual password to get login although this process is complex .So the graphical password comes into the picture it provide us more security than the text based password.

Graphical password is categorized into two parts: Recognition based technique and Recall based technique. Recall based technique is broadly divided into two parts pure Recall based technique and Cued recall based technique.

Recognition Based Technique

In recognition based technique user has to recognize or reproduce the password in the login session which he/she created in the password creation. If user successfully recognize the password images which he//she given in the authentication process the user gets successfully logged in. Khot paper is based on Recognition based graphical password it basically works on WYSWYE(Where you see is what you enter)strategy, where the user identifies a pattern of password images within a presented grid of images and replicates it into another grid this technique prevents user from shoulder surfing attack.

Passface is one of the RBGP where images of human faces for login is taken but limited number of faces is taken into consideration, also user is familiar with the known faces only .

Although this technique takes more password space. Dhamija and perrig[8] proposed a graphical password authentication scheme which is based on hash visualization technique[9] ,In this system the user is asked to select a number of images from a set of pictures and in the authentication process user is required to identify the preselected images.

Pure Recall Based Technique

In pure recall based technique user has to recognize their password without any hints.
Goldberg[10] developed a pass doodle algorithm, graphical password is composed of handwritten designs are text , which is drawn on the stylus onto a touch sensitive screen, study shows that users were able to remember complete doodle images but they were not able to recall the complete order of images .Another pure recall based technique is Draw a secret(DAS),in this technique user has to draw a image from a single movement of a pen so the password is define by a sequence of pen movement but in this scheme most of the user forget their order of pen movement. Another pure recall based technique is Grid Selection in which user first select a drawing grid from much larger grid. Then they zoom it and create a password based on original DAS scheme. The location of chosen drawing grid adds the complexity as there are thousands of possible drawing grids within the selection grid. This scheme just adds the DAS password space but lack of DAS is not yet solved. In 2007, Qualitative DAS method designed in which starting cell and sequence of qualitative direction change in the stroke relative to the grid but this model have more entropy.

Cued Recall Based Technique

In this method, users are given the hints, reminder or gesture to reproduce their password. In 1996,Greg.E Blonder designed a scheme in which a pre-determined image presented to the user and user should point one or two position of the image in a predetermined order but the problem of this scheme was the number of predefined click regions was small and click object should be simple for example cartoon like images. Another scheme is passpoint, in this scheme any pixel in the image offer themselves for examination for a click point so there are hundreds of possible memorable points in the image, but learning is difficult and login time is also more. Another such technique is Passmap in which map of Europe is given to user to select the password from that map and it is easy for user to memorize but a single new edge in a large graph or absence of some edge in the map is not a trivial task .

GRAPHICAL PASSWORD SECURITY ASPECTS

Based on the International attacks patterns standard (CAPEC 2011) as well as related research, at present there are seven common graphical password attacks, namely:

Shoulder Surfing Attack: Attackers can look over the users shoulder in order to find out the password. It is the most important security aspect in which anyone can stolen the password who watch whole login session by peeping over the shoulder or monitor the login with the hidden camera.

Guessing Attack: In this type of attack guesses the password by using users some personal information like mobile number, pets name, friends name. Guessing attack fall into two category: user specific and user generic. User specific attacks like social engineering or knowledge of a user.
Social Engineering Attacks (SEA): In this type of attack attacker can find out the authorized employee information by some other employee. This type of attack is basically defined for an organization. Where the employee's information is stolen and then tries to correlate their information with their password.

Brute Force Attack (BFA): In this type of attack tries to find out every possible combination of password in order to break it. Although this type of attack is generally hard because making combination of total number of digits in password is not so easy and it is time taken also.
Dictionary Attack: This method checks words in a preset dictionary and test whether they used as a password or not.

Spyware attack: Spyware installed themselves on user's computer and they records sensitive data.
Observation Attack: Complete password is visible on the screen during login session. It is ease of viewing and interception of authentication communication between server and client. It may cause the phishing attack.

PROPOSED SYSTEM

The proposed system is based on Recognition based graphical password that not only resist the user from shoulder surfing attack but also from observation attack and guessing attack. The proposed system is based on WYSWYE (where you see is what you enter) strategy. The proposed system works on the grid of images where user is given two grids one is larger grid of images and another is smaller grid. First user has to enter the username and password in the closed environment and register them. In order to login, user first enter his username and then mentally eliminate that row and column which does not contain password images from the larger grid again repeat the same process then map the password in the smaller grid every time the sequence of password images changes which appears to the user so it resist from shoulder surfing attack.

EXPERIMENTAL RESULT

In Fig. 1 this module, user has given two choices one is to use account and if user is new then it gives choice to register itself by clicking on new user button user first register them by giving his user name and password and use account option is for existing user.

In Fig 2. It is used to set the username. The user name is unique for example figure 1: shows the first module result such that user name is nov123@yahoo.co.in and then select the password from the gird of images in the example password image is dog, owl, goat and yak. This process is conducted in secure environment; in this case user selects his username and password images after clicking on ok button user has given unique number for future use. In the list of 36 images user has to select only four images as his/her password. Password may be combination of alphabet and digits also.

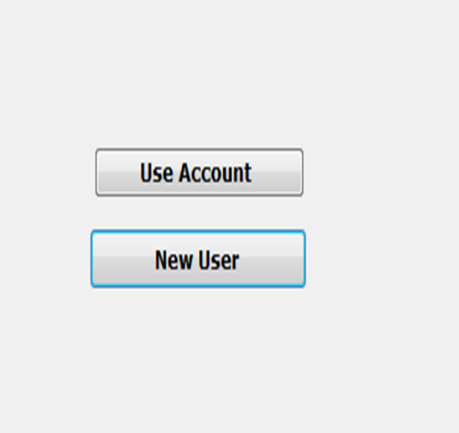

Fig 1: User is given two choices

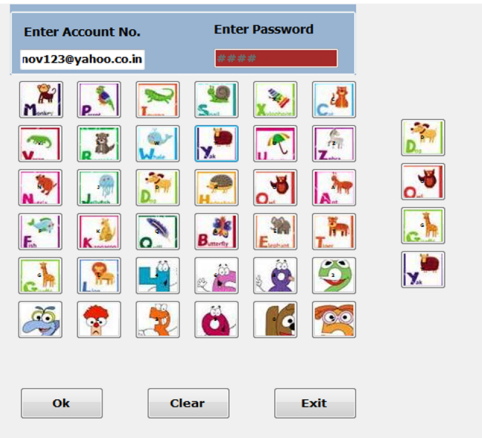

Fig 2: after selecting user name

In fig. 3 this module user enters his unique number that is given on the registration time.

Fig 3: Unique number is given for elimination

Fig 4: Elimination of row and column

In fig.4 this module the row and column is eliminated mentally. Elimination of row and column is done from top and left side. In fig 5 this module the previous step is repeated again and the position of the password image is also changed, then mapped the image into the blank grid. In fig 6 Finally map the password into a blank grid. Mapping sequence is not so important if user correctly maps the password images then user is authenticated.

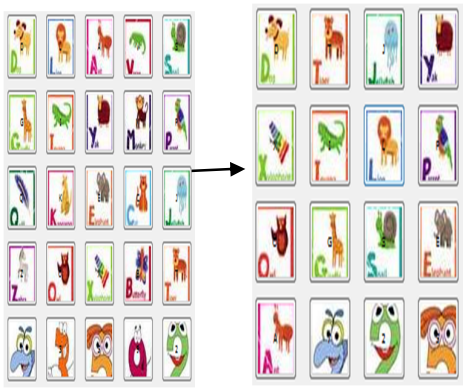

Fig 5: Elimination of row and column again.

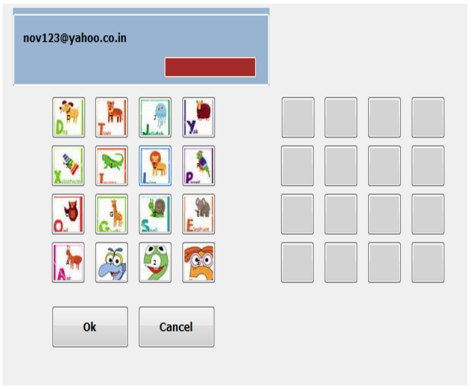

Fig 6: Mapping of password

USABILITY EVALUATION

We conducted controlled laboratory experiment to check the usability of the system. Every participant was assigned the experimental conditions. In this system, user is given image grid of larger size then mentally eliminates row and column which doesn't contain password images apply this process two times then map the password on blank grid.

Participants

30 participants were involved in our experiment, 21 female and 9 male. Before starting the experiment , we collected basic information of all the participants, which include name, age, educational background and knowledge about graphical password. The youngest participant was 17 years old and oldest was 42 years old. Seventy six percent of the participants came from technical background and rest twenty four percent of participants came from non technical background. None of the participants has knowledge of graphical password.

RESULT

The results are based on 90(30 participants * 3 login session), authentication sessions performed by 30 participants. Results is based on Accuracy (Success rate of login), Efficiency (Time taken for login).

Accuracy

We first test whether a participant could login to the system within three trials. Accuracy is measured in first day, after fifteen day. In the first day every participant signs in to the system with their email ID and password. First day more than 92% of the participants successfully login to the system. After fifteen day we again test the system and more than 80% of the participants successfully login to the system in first trial and more than 12% of the participant's login in trial 2. We measure the accuracy in terms of login to the system by remembering the password images as shown in figure 7 and 8 the success rate in first and fifteenth day.

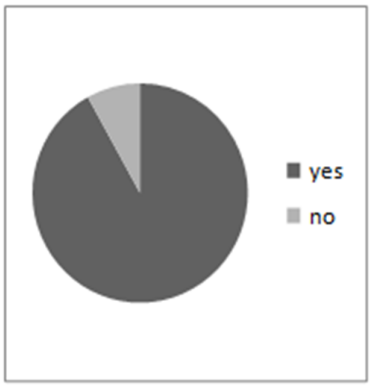

Fig 7: First day success rate in first trial.

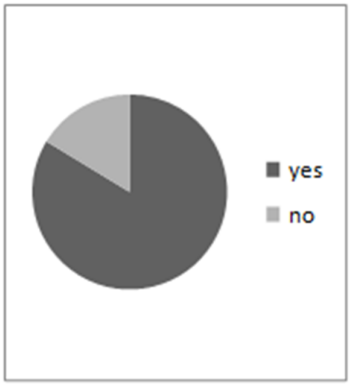

Fig 8: Fifteenth day success rate in first trial

We observe that login success rate is more in first day and reduced in fifteenth day. All participants login to the success in maximum three trials. As shown in table 1 approx 90% of user login to the system in first trial only but rate is reduced in fifteenth day. Success rate increases with practice because most of the user not familiar with graphical password.

Table 1. Total no of participants who required attempts to login for the three trial (n=30)

Trial / Day	Trial 1	Trial 2	Trial 3
Day 1	27	2	1
Day 15	24	4	2

Efficiency

We observe the login time in all the three trial. The scheme shows the slow login time average mean time of the system and average standard deviation (mean: 40, SD: 2.7)

USER SATISFACTION

In the study, we collected the user responses on easy to remember, user friendly, Interactive, security, confident in using the system. Eighty percent of the participant easily remembers the system. Seventy eight percent of the participants found system user friendly. Seventy five percent of the participant fined this system interactive. Ninety percent of the participants said system to secure and they willing to use the system in future. Eighty percent of the participant's confidence on using the system. Figure 9 shows the Responses show high level of security.

SECURITY EVALUATION

There are two ways in which an attacker can try a system. First, attacker can try to randomly guess the password (four images as the password). In this scheme the grid contains 36 different images out of which four image contains password since order is not important so, here are 58,905 possible combinations of choosing four images out of presented thirty six images($^{36}C_4$). Therefore probability of a single random guess of password is 1⁄58,905.

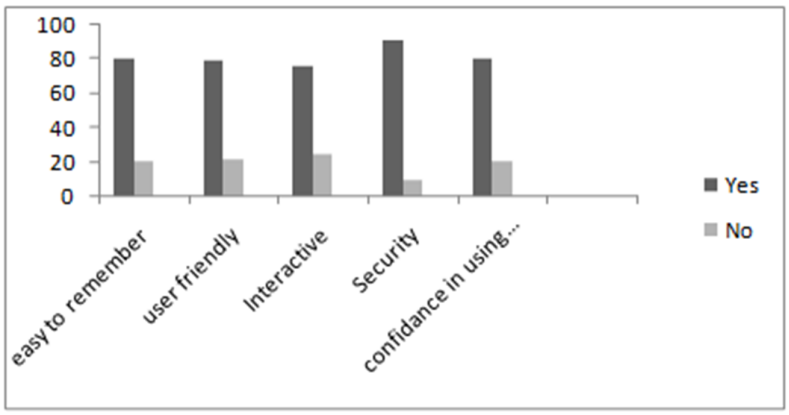

Fig 9: Responses show high level of security

Alternatively, attacker can randomly guess the one time password from the mapping position of the password. User can mark any four blank grid from 4*4 grid so probability of guessing the password is 1⁄1,820 ($^{16}c_4$). Since for every session position of password changed so brute force attack is not feasible. In WYSWYE paper the password space is 12,650 so probability of guessing the password images is higher than DASSA scheme because in this scheme password space is 58,905 which is much higher than 12,650.

In table 2, proposed scheme is compared with the Khot(DR) WYSWYE paper as in the challenge grid proposed scheme has 36 images where in Khot(DR) WYWYE has 25 images so password space is more in the proposed scheme.

Table 2. Comparison of paper

Scheme	Challenge grid	Password space	Password space for one time password
Khot(DR) WYSWYE	5X5	12,650	1,820
Proposed scheme	6X6	58,905	1,820

Shoulder Surfing

In this scheme, user cannot directly clicks on the password images but selects the random images so if user watch the login session from hidden camera or from peeping over users shoulder cannot guess the password and every time the position of the password images changes so shoulder surfing attack is not possible to this system.

CONCLUSION

This system will resist against shoulder surfing attack, in this system every time user enters the password and the position of password images changes every time so person standing before can see the password but cannot guess for the password, at the time of mapping of the password the mapping sequence is not compulsory so probability of guessing the password is very less this system will resist against the observation attack, because anyone who is monitoring the login process can not directly see the password because the elimination of row and column is done mentally .

FUTURE WORK

We can apply different types of images on it and then eliminate rows and column or on human faces because people can remember faces more easily.

REFERENCES

Dunphy,P.,Fitch,A.,and Olivier,P.Gaze "Contingent graphical passwords at the ATM ," In Proc.COGAIN'08.

Jakobsson,M.,Shi,E.,and Chaw,R."Implicit authentication for mobile devices",In proc.HotSec 2009 .

Rohit Ashok Khot , Ponnurangam Kumaraguru , Kannan Srinathan,"WYSWYE: Shoulder surfing defense for recognition based graphical password," *OZCHI'12, ACM*, 2012.

Arash Habibi ,Lashkari,Farnaz ,Towhidi, Dr. Rosli Saheh and Samaneh

Farmad"A complete comparison on pure and cude recall based graphical User authentication algorithms",IEEE,2009.

Uma D.Yadav,Prakash S.Mohod"Adding persuasive features in graphical password to increase the capacity of kbam",International Conference on Emerging Trends in Computing, Communication and Nanotechnology,IEEE,2013.

Ruhi kaur oberoi,vivek P kshirsagar"RAS-advanced security using gui password", international confence(pune)IRD-2012.

H.Zhao and X.Li,"S3PAS:A scalable shoulder surfing resistance textual graphical password authentication scheme",Proc.of 21st Int.Conf.on Advanced Information Networking and Applications Workshops,vol.2, ,pp.467-472, May 2007.

R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX secuity symposium 2000.

A. Perrig and D. Song, "Hash Visualization: A New *Technique to improve Real-World Security," in proceeding of the International workshop on Cryptographic technique and E-commerce 1999*.

Hristopher Verenhorst,"Passdoodles;a lightweight Authentication Method",Massachusetts Institute of Technology,Research Science Institute,july 27,2004.

Arash Hbib Lashkari,Azizah Abdul Manaf,Maslin Masrom"Graphical password security evaluation by fuzzy AHP",world academy of science,Engineering and technology 2012.

Rosanne English,Ron Poet"Towards a metric for recognition based graphical password security", IEEE ,2011.

Arash Habibi Lashkari,Azizah Abdul Manaf,Muslin Masroom"Graphical password security evaluation by fuzzy AHP",World Academy of science, Engineering and Technology 66 2012.

Yi-Lun Chen,Wei-Chi Ku,Yu-Chang Ye,and Dun-Min Liao"A simple text based shoulder surfing resistant graphical password scheme",National Science Council,Taiwan.

Daniel Ritter,Florian Schaub,Marcel Walch,Michael Weber"MIBA:Multitouch image based authentication on smartphones", CHI ,Paris,France ACM 2013.

A. S. Patrick, A. C. Long, and S. Flinn, "HCI and Security Systems," *presented at* CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA. 2003.

R. N. Shepard, "Recognition memory for words sentences, and pictures," *Journal of* Verbal Learning and Verbal Behaviour, vol. 6, pp. 156-163, 1967.

Xiaoyuan Suo, Ying Zhu and G. Scott. Owen, "Graphical Passwords: A Survey", Proceedings of the 21st Annual Computer Security Applications. IEEE, 2005.

Brostoff, S., Inglesant, P., and Sasse. M. A, "Evaluating the usability and security graphical one-time PIN system," 24th Conference on Human Computer Interaction *HCI, pp 88-97,*ACM, September 2010.

Panjwani, S., and Cutrell, E. Usably secure, "low-cost authentication for mobile," In *SOUPS* ACM, 2010.

Weinshall, D. Cognitive "Authentication Schemes Safe against Spyware," In Proceedings of the IEEE Symposium on Security and Privacy, May 2006.