STRENGTHENING PASSWORD USING ER IMAGE MATRIX MODEL WITH PCCP BASED GUI SCHEME

S.Uthayashangar
Assistant Professor,
Dept. Of Information Technology,

R.Srinivasan
PG Scholar,
Dept. of CSE

Jayamoorthy.S
Assistant Professor
Dept. of CSE

Manakula Vinayagar Institute of Technology, Puducherry.

Abstract: Today many security algorithms have been implemented for providing security towards users' personal data. So maintaining strength of the password is challenging role. Usually passwords are created by text only. But it has vulnerability. So last few years we slightly move towards picture based security authentication is called PGA (Picture Gesture Authentication). It also has possibility to vulnerability because the hacker once identified the sequence of image. But our proposed scheme has little bit additional towards security called ER with PCCP. The ER (Entity-Relation i.e., One-to-One, Many-to-Many, etc.,) with this sequence of image selection at the end user can draw the click-point at the final image. If the user correctly enters the sequence the system must allow to access the data otherwise it shows "incorrect access". In this way additional security must be provided towards PCCP based system by using ER model. We show that our system will perform better in terms of speed, accuracy and better security.

Key Index: PGA (Picture Gesture Authentication), ER (Entity-Relation), Check-point, constraints, PCCP (Pervasive Cued Click Points)

I. Introduction

Many security algorithms and security based schemes such as Integrity, Authentication, Authorization; Encryptions are designed to provide the security. But still Hackers / Attackers have guess the password to break the security scheme. In General we use Text Password for security. But it has possible to vulnerable. So Last few years we slightly move towards Image based security. It has been implemented effectively with the help of concept PCCP. In this, scheme has the maximum possibility to click points on Image to break the password at the Raster Image. In this paper I had little bit extend the security using PGA (Picture Gesture Authentication) with E-R model. In general, ER are implemented in rule based system with which security semantics constraints i.e., cardinality relationship as one-to-one, one-to-many, many-to-one & many-to-many scheme the security password must come under any one constraints as described while these scheme is implemented (the first check point is) when the user enter the username followed by the first check-point is to select the user constraints i.e, select anyone among the three. After selecting any one constraint the sequence to be entered one after another followed until the last sequence must match the password of the username. If the sequence must mismatch with original ordered sequence at the third time the user-id data will be blocked. So that one maximum possibility of reducing the network attack can be reduced.

Today, Data Transmission through communication network has wide range. But the security mechanism adapted towards the communication schemes are often broken by the hacker. The main intention of the hacker is to break the "password" of any security block. But user has to provide better security for each and every time when additional secure mechanism is implemented inorder to communicate the secret shared data between the parties. Here we noticed even though the tough password can be used by the user but still some crucial mechanism is finding out by the user. We known the texture based password breaking mechanism such as Back Shoulder surfing, spoofing,

malware, spyware, etc. to crack the password and attacker to achieve their intention to hack the data. In order to overcome those attacks happened by using texture based password. We slightly move towards the image/picture based password has to reduce the attack by half. The graphical password has the enough security but still it has the disadvantage of attacker to know the click-sequence of identifying the image. So, in our proposed method the graphical password scheme we slightly move towards PGA with ER model security implementation is a new way of trying security authentication for the password scheme.

Here, a new and novel way of handling password instead of texture, the Graphical Passwords are used because Psychology studied that human brain can recognize images better than the text. So assigning the graphical passwords the user must aware of maintaining the security more when compared to text. Because the Back Shoulder Surfer and some network hacker can guess the images of the users password while the minimum usage of Images as input password images. So, in order to improve the security over this GPS (Graphical Password Scheme) the user can little-bit extent the scheme towards PCCP (Point Cued Click Point). In this model the point-click on the image is at one point on single-image is guessed by attacker then there may be a possibility to break the password.

But, in our proposed approach the multiple-image with multiple stage by using ER based model, which is used depending upon the user accordance i.e., with minimum of 8x8 or 16x16 matrices of images along with PCCP process is implemented at the final image selection process the security mechanism decides the authenticated user . So, by implementing this scheme we will provide more security than previous scheme. But one drawback of this scheme is large processing time needed for the system to identify the exact user of an login system and large memory space for storing the images of each individual user password images. Even though these latency but it overcomes the guessing and breaking of original password is slightly more difficulties for the malicious user. So, this scheme is much more confident towards to the new users who are really making want to keep their data more secure in the real-world user. This paper also includes II. Background, III. Proposed System, IV. Implementation & V. Conclusion.

II. Background

Previously various Graphical Password techniques were introduced. Some of the techniques are given below, *Pass-point Scheme* S. Wiedenbeck et al. [6] [8] [9] proposed pass-point graphical password scheme in which on a given image password consists of a sequence of 5 different click points. For password creation user selects any pixel in the image as a click-points and for login the user has to enter the same series of clicks in correct sequence within a system defined tolerance square of original click-points. The problem with this scheme is the HOTSPOTS [11][12](the area of an image where user more likely to select the click-point) and it is easy for attackers to guess the password because user forms certain patterns[13][14] in order to remember the secret code which results pattern formation attacks are easily possible.

Fig 1: Pass-Points

Cued Click Points

In the above pass point scheme, instead of five click-points on one image, CCP uses one click-point on five different images. The next image displayed is based on the location of the previously entered click-point; it creates a path through an image set. Creating a new password with different click-points results in a different image sequence. One best feature of Cued Click Point is that the explicit indication of authentication failure is only provided after the final click-point, to protect against incremental guessing attacks.

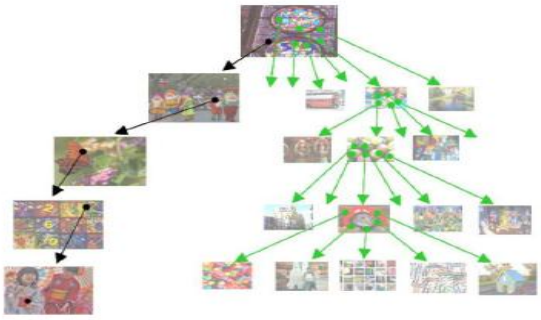


Fig. Cued Click Points

Persuasive Cued Click Points

The advantage of CCP over PCCP is added extra feature towards the CCP as PCCP uses concepts like viewport & shuffle of Images randomly while the user select the password Images. At the same time the PCCP challenges the attackers have to improve their gausses. Then user has to select correct click on particular image. PCCP is a good technology but has security problems. Fig. shows the password creation process including viewport & shuffle button.

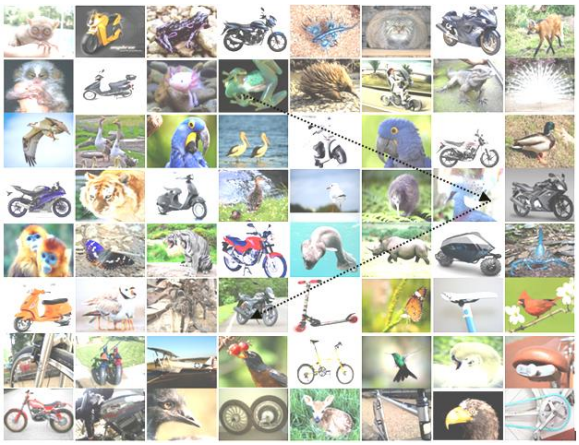


Fig. password creation in PCCP.

Click-Draw Based Graphical Password Scheme

The purpose of click-draw based graphical password scheme (CD-GPS) [3] is to enhance the image-based authentication in both security and usability. There are mainly two steps in this scheme: 1. Image selection, 2. Secret drawing.

1. Image selection

In CD-GPS, the first step is the image selection. In this step users have to select several images from an image pool. The user has to select the image according to their ER based relation from the image pool. After this process is over, it moves to next steps of one-to-many relationship towards the next level of image pool for selecting the particular image among the matrix of images. This process called image selection.

2. Secret drawing.

After the completion of image selection process the next step is to draw the secret image. Here user can freely click draw their secrets so that the redrawing the same secret image by unauthenticated person can draw as possible when he accurately draw in the correct coordinates of images so it also has more possibilities to attack.

III. Proposed System

In this paper we proposed a system called ER model with PCCP scheme for providing better security towards users. The PCCP & Click Draw Based Graphical Password Scheme has finally deployed at the end-process of ER-model. The ER-model security scheme is implemented in 3 levels scheme at each level, the user confidential must be authenticated and exact end user only can access the system.

The levels are

(i) Sequence of One-to-Many Image Selection.
(ii) Sequence of Many-to-Many Image Selection
(iii) Final User Click-based Image Vs PCCP

(i) Sequence of One-to-Many Image Selection

The initial level of Image Selection under this scheme the user must enter the username and select the first image of password under Image Pool where the user already selected as the password images under the ER-model.

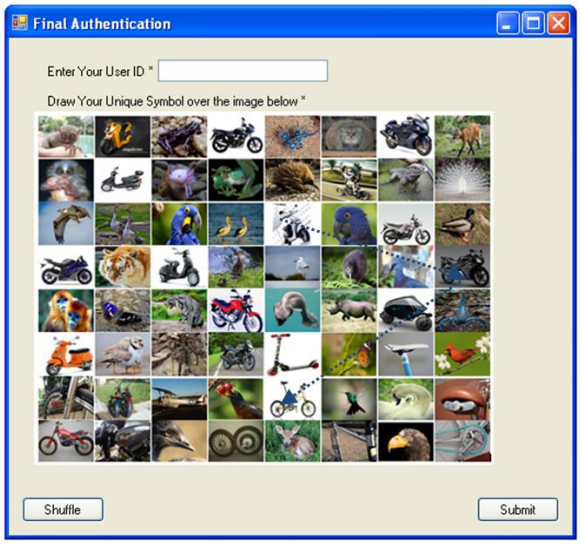
After selecting the image from level 1 image pool, the user must select the Entity-Relation Based Image at the next matrixes of Image. Here Each and Every row & column of Image has Inter-logically dependent on the next image i.e., one among Image where the many-to-many relationship exists between the Entity Image. So, that third-party guessing of images among the E-R images is very low while because the user only known that scheme of our authentication. While the 3rd person selecting the level-1 initial stage to many images the possibility of selecting exact images among the random persuasive image in order to avoid the known hotspots, the viewport & shuffle. So at the initial level itself we have up to 30% achieve security. And the next step process is involved.

(ii) Sequence of Many-to-Many (One) Image Selection

In this stage of selecting Image Based on not only on the current image features selection it will depends upon the Level-1 stage of Images from 16x16 pixel image pool. Here only we are going to implement the Entity Relation features. So, in this stage once again one-to-many concept is implemented so that next step of selecting the desired picture/image among the set of 16x16 Image pool. But picture is not always in the exact location as original state/position it was randomly moved among the location by after clicking level-1 set of initial selection of the first image. So, the password i.e., Image Guessing/Hacking the sequence between the image selection processes is to a tidy to the new users. Here we additionally provide the change the real-user who is never forget their password even he entered to select images from multiple stages from different paths. Because user has to remember their sequence as their wish with some intra-inter relationship between the objects/ (Images) Entity Selection. At the same time the password cracker has to guess the image of original password image he is not select the level-2 password image select is exact images as original image of this state so possibility of attack is less and this level the security goes up to 70%.

(iii) Final user Click-based Image Vs PCCP:

After finishing level-1 & level-2 Image Selection process. The last and final step for providing maximum % of security towards this scheme is called Level of Contingency or Level of Satisfaction/dissatisfaction about the exact user.



Select the image so that after level-2 image selection process completed the single image form image pool at this image has two levels as: (1) Image selection, (2) Secret drawing as already explained. During this Entire process we set the goal for excepted user with some time clock period with possibility of providing maximum attempt of 3 chances for all states of selecting the exact image at desired stage. Through this way the correct or

authenticated user has not lose their maximum possibility to utilize the data. But for the inexperienced or new user can definitely loose the maximum possibility at some level so that the high-level security can be implemented using this ER-based PCCP.

IV. Implementation

Consider one example illustration to show how long our implementation provide security towards the passwords as explained step by step process as below. During the initial state the user has to select the picture/image in a vertical form in our example i.e., person, tow wheelers, animals. After selecting any one (i.e. person) among that next it will automatically go to ER- based pre-defined matrices of picture with 8x8 images in that level-1 stage any one image ie., I am going to select baby this process we said as one-to-many process. After the correct image is selected it will be redirected to next stage ie., we called Many-to-One selection process called level-2 stage.

Here according to my example Two wheelers has 8x8 attributes related to that particular images i.e., {Tvs50, Scooty, Activa, Pep, Streak, Bicycle, Honda, Yamaha, etc…} among the tuple the correct user can select the exact image so that after clicking that image by the user the next process is to draw the secret image on the finally selected image so that it verify the trustiness of user who is login into their own block to access the data. If the user draw it correctly it automatically allowed to access their data otherwise it will rejects at the end-state. During miss-selection of any images at any levels it will redirect to next state but it not watch with the exact user with exact entity of tuples with exact secrets drawing at the end state image. So, this provides more security towards the valid user who is maintaining utmost security towards their password as secrets.

The system is not trusting the user at every state so that it will analysis the activity of the user with its database it those possibilities of mistakes exceeds more than three times of selecting each & every stage of images selection than it will reject that particular users username based database to block the whole. But some extent the authenticated user can itself exceeds the needed criteria that will not allows to draw the click-based images before that it will ask some security questions to trust it if the user answer it correctly it will allow to access or else it finally hide the entire image it shows the blank white image it shows that “U R NOT ALLOWED TO ACCESS THIS PAGE”& You have entered incorrect password/sequence. Try again”.

V. Conclusion

Our proposed scheme has various advantages such as hard for the attacker while guessing the password i.e., Image at some level of sequence during ER-Model process because, the authenticated user can utilize the possibility choice exactly to maintain data secrecy so that the strength of password is also very high. At the same time the disadvantages of this ER- model with PCCP password processing and matching with exact sequence for every authenticated vs. unauthenticated user satisfaction and dissatisfaction process of taking decision is little tedious. And additional memory requirements need for processing each user with maintaining individuality. Clicking the click-point at end-image we provide the (color histogram) with user favorite color selection with the generated waves. The wave generation & color sequence is random process of generating one not a default one.

V. References

[1] "Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme", P. R. Devale Shrikala M. Deshmukh, Anil B. Pawar, International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-3, Issue-2, May 2013.

[2] "Image Authentication in PCCP through Click-based Graphical Password", Radhika. G, Maximus Sowndarya Jhonsy. R, Chandhini Mona. J, Uthayashangar. S.

[3]. “Persuasive Cued Click-Points: Design, Implementation and Evaluation of a Knowledge-based authentication mechanism”, IEEE Transactions on Dependable and Secure Computing, 2012.

[4]. S. Chiasson, R. Biddle, and P. van Oorschot, second look at the usability of click-based graphical

passwords," in ACM Symposium on Usable Privacy and Security (SOUPS), July 2007.

[5].E. Stobert, A. Forget, S. Chiasson, P. vOorschot, and R. Biddle, "Exploring usability effects of increasing Annual Computer Security Applications Conference (ACSAC), 2010.

[6].S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "User interface design affects security: Patterns in click-based graphical passwords," International Journal of Information Security, Springer, vol. 8, no. 6, pp. 387–398, 2009.

[7].S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using Cued Click Points," in European Symposium on Research in Computer Security (ESORICS), LNCS 4734, September 2007, pp. 359–374.

[8].S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle, "Multiple password interference in text and click-based graphical passwords." in ACM Computer and Communications Security (CCS), November 2009.

[9].S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot, "Influencing users towards better passwords: Persuasive Cued Click-Points," in Human Computer Interaction (HCI), The British Computer Society, September 2008.

[10].S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot, "User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords," Int'l J. Information Security, vol. 8, no. 6, pp. 387- 398, 2009.

[11] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The Memorability and Security of Passwords," Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, eds., ch. 7, pp. 129-142, O'Reilly Media, 2005

[12]. S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.

[13].S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot.Influencing users towards better passwords: Persuasive cued click-points. In Human Computer Interaction (HCI), The British Computer Society, September 2008.

[14].S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot. User interface design affects security: Patterns in click-based graphical passwords. Technical Report TR-08-14, Carleton University, 2008.

[15].J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The memorability and security of passwords," in Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, Eds. O'Reilly Media, 2005, ch. 7, pp. 129–142.