Captcha as Graphical Password for User Authentication: A New Security Primitive

[1]P.Lavnya, [2]R. Sivaranjani
[1]Student of M.Tech, CSE, GMR Institute of Technology, Rajam
[2]Associate Professor, Department of CSE, GMR Institute of Technology, Rajam

Abstract *- Most of the computer systems use password as a method of choice for authenticating users. Text is generally is used for such authentication, but these text-based passwords are insecure.To provide a better security for user authentication Captcha (Completely Automated Public Turing tests to tell Computers and Humans Apart) as graphical passwords are used. Graphical passwords use images or representation of images as password. The human brain easily remembers the 'Graphical image secret word' when compared to the 'Text secret word'. Now-a-days, in market, many graphical image secret word software's are available, as well as distinct graphical image secret word methods. The work proposed in this paper, merges Cued click points with token based verification and Captcha text. Prime intention of this proposal is to minimize the guessing attacks as well as to encourage users to select more-random and difficult-to-guess passwords.*

IndexTerms— Password, Graphical password, CaRP, hotspots, Captcha, password guessing attack, dictionary attack, security primitive.

I. INTRODUCTION

In earlier days, text-based passwords are used for authentication. Text-based passwords' authentication is nothing but a string of alphanumeric characters. Users always create a password which is easy to remember, but these passwords are also easy to break for attackers. To ensure more security, users started the use of strong 'system assigned passwords', which were difficult for users to remember. As an alternative for this, graphical passwords [1, 2] are used because psychology studies state that human brain can recognize images better than the text.

Graphical passwords [1, 2] are of three types: Click based graphical password scheme [8], choice based graphical password scheme and draw based graphical password scheme. In this proposed work, user clicks on sequence of five images. At the time of login phase images appear as per the random sequence. In the registration phase, user selects 5 images from the image pool or local drives. While users coming to login phase, select images from the image pool based on image selected by registration phase and then click on images for click points. If both the click points' distance is below a tolerance value then it is allowed. Otherwise abort the user. Click points values of all five clickable images will be used for calculating Euclidean distance. This Euclidean distance is compared to a particular tolerance value. This proposed system provides three-way authentication and also provides higher security than other techniques.

II. BACKGROUND

There are several Graphical image Password methods [1, 2] were introduced. Few of those techniques are explained below.

A. Pass-Points

S. Wiedenbeck et al. proposed pass-points [3] graphical password scheme image password consists of a sequence of 5 different click points on single image. 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. Main drawback with this method is the HOTSPOTS - 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 in order to remember the secret code. This makes 'pattern formation attacks' easily possible. This method endures from these two major problems. To overcome these problems next method was implemented

Fig. 1. Pass Points System

B. Cued Click Points

'Cued Click points' method was designed to reduce patterns [7] and to reduce the usefulness of hotspots for hackers. In preference to five click points on one single image, CCP uses one clickable region on five distinct images. The next new image presented is based on the location of the previously entered click point. It creates a path through an image set. Best feature of the Cued Click Point is that the explicit indication of authentication failure is only provided after the final click point, to define beside accumulative guessing attacks. But this method also has more drawbacks like false accept (the incorrect click point can be accepted by the system) and false reject (the click point which is to be correct can be rejected by the system). In this existing method pattern realization attack is reduced but HOTSPOT remains since users are selecting their own click point.

Fig. 2. Cued Click Points System

C. Persuasive Cued Click Points

For creating Persuasive Cued Click Points [5, 6] persuasive feature is added to CCP. PCCP encourages users to select less probable passwords. For password generation PCCP uses requisites like viewport & shuffle. When users making a secrete word, the images are a little monochromic except for a viewport for to avoid known hotspots the viewport is positioned casually. The most useful benefit of PCCP is hackers have to improve their presumptions. Users have to choose a clickable area within the highlighted viewport and cannot click outside of the viewport unless they press the shuffle button to randomly reposition the viewport.At the time of password creation slows the process of password generation. Only during the password generation, the viewport & shuffle buttons are displayed. After the secrete word generation process, graphical images are presented to users casually without the viewport & shuffle button. Then user has to choose exact clickable area on particular image. Now a day's PCCP is a best technology but has security problems.

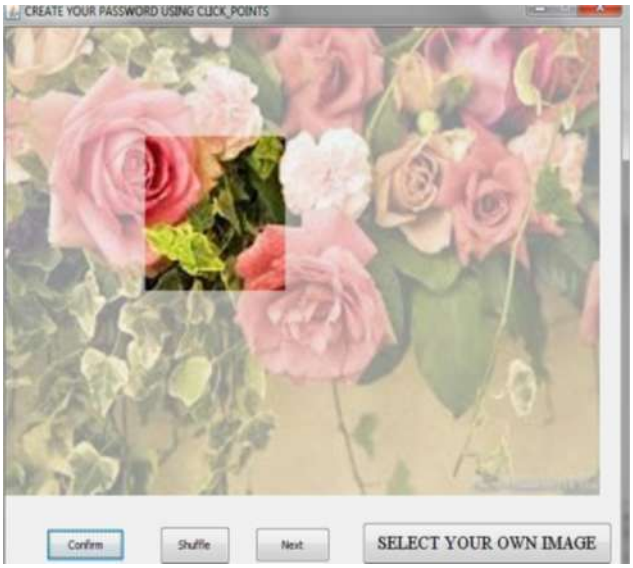

Fig. 3. Persuasive Cued Click Points System

Figure.3 shows the password creation process including viewport. Using this method HOTSPOT problem is reduced, but this method is difficult to remember the exact clickable area.

D. Captcha

A CAPTCHA [10] (Completely Automated Public Turing test to tell Computers and Humans Apart) is a computer program that can generate and grade tests that: (A) most humans can pass, but (B) current computer programs cannot pass. Such program can be used to distinguish humans from computers and determine whether or not the user is human.

E. Captcha in Authentication

A User Authentication Protocol, termed as *Captcha-based Password Authentication (CbPA) protocol*, was introduced where both 'Captcha and Password' are used to counter online dictionary attacks. In CbPA-protocol, it is required to solve a Captcha challenge after inputting valid pair of user ID and password, unless a valid browser cookie is received. If an invalid pair of user ID and password are entered, the user is prompted to solve a Captcha challenge before being denied access. An improved CbPA-protocol is proposed in by storing cookies only on user-trusted machines and applying the Captcha challenge only after the user exceeds the threshold number of failed login attempts for the account. It is further improved in by applying a small threshold for failed login attempts from unknown machines but a large threshold for failed attempts from known machines with a previous successful login within a specific time frame. Captcha was also used with recognition-based graphical passwords to address spyware, wherein a text Captcha is displayed below each image; a user locates his/her own pass-images from decoy images, and enters the characters at specific locations of the Captcha below each pass-image as his/her password during authentication. These specific locations were selected for each pass-image during password creation as a part of the password. Captcha is used to protect sensitive user inputs on an untrusted client. This scheme protects the communication channel between user and Web server from keyloggers and spyware.

III. EXISTING SYSTEM

Existing System is based on recognition techniques where methods like 'ClickText' [1] and 'Animal Grid' [1] are being used. In this method, firstly user-registration is done and then ClickAnimal image is displayed and user clicks any one of the animals. At the time of login, user must click on the same animal in the ClickAnimal image. These methods are elaborated below.

***A.ClickText*:** *ClickText* [1]is a CaRP scheme built on top of text Captcha based on recognition and its alphabet consists of characters without any visually-confusing characters. For example, letter "O" and digit "0" may cause confusion in CaRP images, and thus one of characters should be excluded from the alphabet. A ClickText password is a sequence of characters in the alphabet, e.g., ρ ="AB#9CD87", which is comparable to a text password. A ClickText image is generated by the underlying Captcha engine as if a Captcha image were generated except that all

the alphabet characters should appear in the image. While generation, each character's location is traced to produce ground truth for the location of the character in the image thus generated. The authentication server relies on the ground truth to identify the characters corresponding to 'user-clicked' points. Characters in 'ClickText images' can be randomly arranged on 2D space whereas in text Captcha challenges the characters are typically ordered from left to right in order for users to type them sequentially. Figure. 4 shows a ClickText image with an alphabet of 33 characters. In entering a password, the user clicks on this image the characters in his/her password, in the same order, for example "A", "B", "#", "9", "C", "D", "8", and then "7" for password="AB#9CD87".

Fig. 4. ClickText image with 33 characters

B. Animal Grid

In order to enter a password, firstly, a ClickAnimal image [1] would be displayed. Upon selecting an animal, an image of $n \times n$ grid appears with the grid-cell size that exactly equals to the bounding rectangle of the selected animal. Labelling each grid-cell aids users ease to identify.For instance, when the red turkey in the left image of Figure. 5 is selected, a 6 × 6 grid is displayed as shown in Fig. 4. User may select zero to multiple grid-cells matching his/her password. Thus a 'password' is a structure of animals interweaving with grid-cells, e.g., ρ = "Dog, Grid(2), Grid(1); Cat, Horse, Grid(3)", where Grid(1)means the grid-cell indexed as 1, and grid-cells after an animal means that the bounding rectangle of the animal determines the grid. A password always begins with an animal. When a ClickAnimal image appears, user clicks the animal on the image that matches the first animal in his/her password and the coordinates of the clicked point are recorded.

Fig. 5. Click Animal image (left) and 6×6 grid (right) determined by red turkey's bounding rectangle

Then the bounding rectangle of the clicked animal is found interactively as below: A bounding rectangle is calculated and displayed, e.g., white rectangle displayed in Figure.5. The user checks the displayed rectangle and corrects inaccurate edges by dragging, if needed. This process repeats until the user is satisfied with the exactness & accuracy of the bounding rectangle. Usually, the calculated bounding rectangle is accurate enough without needing manual correction. Once the bounding rectangle is identified for the selected animal, an image of $n \times n$ grid, with the identified bounding rectangle as its grid-cell size, is generated and displayed. In case the grid image is too large or too small for a user to view, the grid image is scaled to a size that fits. Then the user clicks a sequence of zero to multiple grid-cells that match the grid.

IV. PROPOSED SYSTEM

A. Introduction

In this system, user selects the number of images to click points on images. At the time of login phase images appear as per the random sequence. In the registration phase, user selects up to 5 images from the local drive. After the images are uploaded user clicks on images for click points. In this up to maximum 5 click points are allowed. Based on the click points on images the points are stored in database. While users coming to login phase, select images from the image pool based on image selected by registration phase and then clicks click points on images.

In this proposed system first generate the application for Captcha authentication system. If the Captcha is entered correctly then only it moves to the image selection. Once the image selection and click points are completed it moves to the user profile page. When creating a password, all clickable points are marked on corresponding image for a user to select. In the course of authentication, the user first enters the captcha, and then clicks the password points on the images. The authentication server finds the closest clickable point on the image by mapping each user-clicked point. Login fails if their distance exceeds a tolerable range.

B. System Architecture

The proposed system consists of 3 modules as shown in Figure.6.It includes Registration module, Captcha generation, Picture selection module, and Login module.

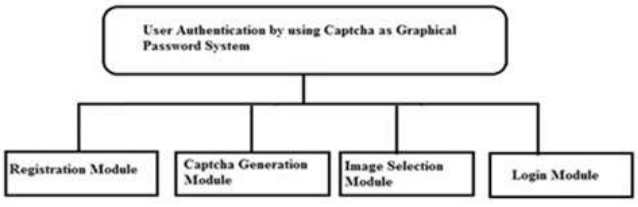

Fig. 6. Architecture Diagram

C. Registration Module

In this module first step is Account Creation which is followed by Password Creation and finally Deciding sequence of images presented or selected. The user has to successfully create his account first. In this system, each user is identified by a unique username. Hence to make sure that each user has a unique username, the system before creating an account checks for the availability of username. If the Username specified by user already exists, then the system prompts for the availability of that name. Once the user name is available it moves to next fields like password, gender, contact number, e-mail, etc. All these fields are stored in database.

D. Captcha Generation Module

In this module a Captcha is generated on an image. The Captcha length is 6, it contains the combination of "A-Z, a-z & 0-9". The Captcha is case sensitive. Once the user enters the correct Captcha text then it moves to the next module. If the user enters incorrect Captcha text then it generates another Captcha. This process repeats until the user enters correct Captcha text.

E. Image Selection Module

This module consists of image selection for click points. Images are selected from local drive. The user can selects maximum of 5 images. Once the images are selected the user can click on images to provide click points. These click points are stored in database.

F. Login Module

The login phase is carried out according to the flowchart shown in Figure. 7.During logging to the Image based Authentication System, the user is presented with the first image which he/she had used during registration time.While logging, the click will not be visible and the user has toclick on his registered click-point on the image.Since it is practically impossible for a person to click on the exact point, hence a tolerance value is hard coded in the system.The tolerance value (D) indicates the degree of closeness to the actual click-point.Euclidean distance is calculated to find the distancebetween two click points. Euclidean distance between two points' p and q is given by

d(p q) = √ (p1-q1)2 +(p2-q2)2+….+ (pn-qn)2 = √Σ (pi-qi)2 i=1 to n

Above distance is calculated for each image and if this distance comes out less than a tolerance value D then only next registered image is displayed. The value of D is taken as 5 in our system.

Thus, if the click-point falls within the system defined tolerance square then only the next correct image will be displayed to the user, else it will displays an error message. The next image displayed is always based on the location of the previously entered click-point, creating a path through an image set. Thus a wrong click leads to an incorrect path, with an explicit indication of authentication failure. Once the user clicks on correct click points it moves to profile page. The profile page contains options for user to edit the data and view the data. If the edits the data the modified data is stored in database.

V. Results and Analysis

A. Results

In this system Captcha and Click Points schemes are used for generating the graphical password. Figure 8 shows the captcha verification for login, once the captcha is entered correctly then it moves to the next page where user first selects the total number of images they are uploaded on registration time. The number of images is compared and if it is correct then the images are displayed for selecting the click points on images. Figures.9 to 13 show selecting 1st, 2nd, 3rd, 4th, 5th click points for password generation.

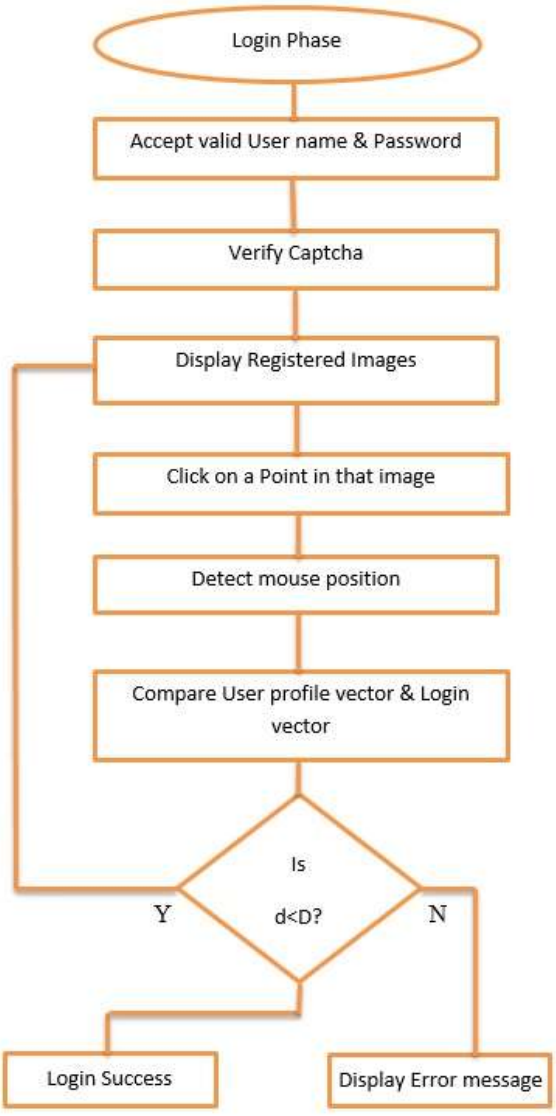

Fig 7: Login Module flow diagram

Fig. 8. Captcha verification

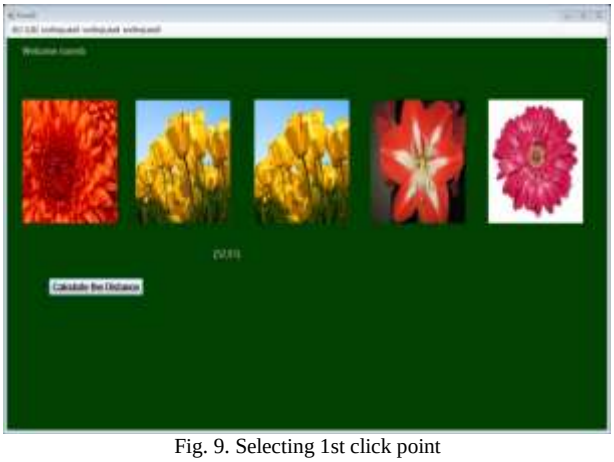

Fig. 9. Selecting 1st click point

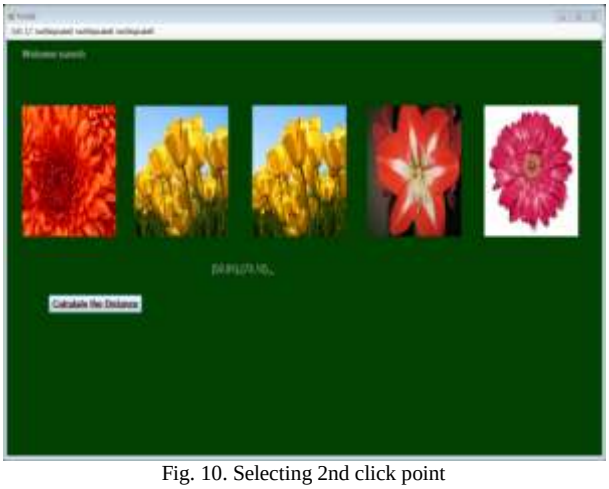

Fig. 10. Selecting 2nd click point

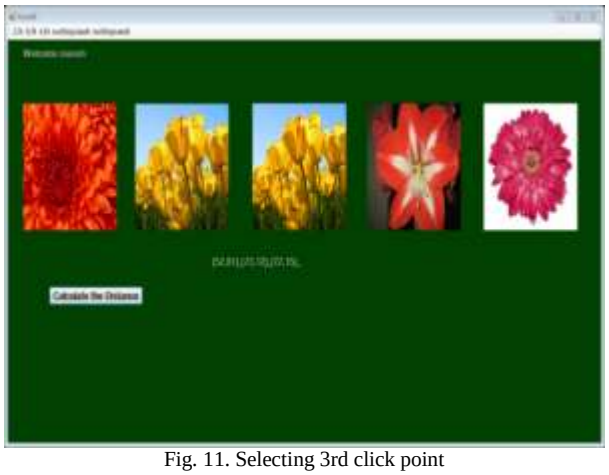

Fig. 11. Selecting 3rd click point

Fig. 12. Selecting 4th click point

Fig. 13. Selecting 5th click point

B. Analysis

The existing system uses ClickText, AnimalGrid and PassPoints [3] schemes. Table1 shows comparison of these schemes maximum and minimum login time in seconds. In ClickText images, characters can be arranged randomly, this is different from text Captcha which characters are typically ordered from left to right, and in

order for users to type them sequentially where as in ClickText users must clicks characters on images. In this system user first enters captcha text and then selects click points on images for login. Table2 shows the login time (in seconds) for different number of selected images. Here the maximum numbers of selected images are 5. Table 3 shows login time for different image sizes. It shows that increasing the size of image will increase the password space but decreases the usability. A major complaint of the users using graphical passwords is that the password registrations and log-in process take too long.

Table 1: Login time for different image sizes

Different Image sizes	Login Time
200X200	2.33
200X150	2.20
168X200	1.54
187X150	1.45
143X135	1.31

Table 2: Login Time (seconds) for Different number of images for click points

Scheme	Click Text	Animal Grid	PassPoints ClickPoints	Captha +
Max(s)	65.62	88.51	45.17	2.33
Min(s)	10.41	13.46	8.36	40

Table 2: Login Time (seconds) for different image sizes

Total number of selected images	Login Time
5	1.52
4	1.40
3	1.25
2	55
1	40

VI. CONCLUSION

We have proposed a new security primitive which uses both – a Captcha and a graphical password scheme. This proposal adopts a new approach to counter online guessing attacks: Images are used for every login attempt to make trials of an online guessing attack, computationally independent of each other.

VII. REFERENCES

[1] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, "*Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems*", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE 2014

[2] Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proc. 8th USENIX Security Symp., 1999, pp. 1–15.

[3] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon,"*PassPoints: Design and longitudinal evaluation of a graphical password system*" Int. J. HCI, vol. 63, pp. 102–127, Jul. 2005.

[4] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surveys, vol. 44, no. 4, 2012.

[5] P.R.DevaleShrikala, M. Deshmukh and Anil B.Pawar. "Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme". International Journal of Soft Computing and Engineering, Volume-3, Issue-2 May 2013.

[6] Iranna A M and PankajaPatil. Graphical Password Authentication using Persuasive Cued Click Point, International Journal of Advanced Research in Electrical,Elecrtorics and Instrumentation Engineering, Vol.2, Issue 7, July 2013.

[7] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, and Paul C. van Oorschot, 2012,"Persuasive Cued Click-Points: Design,Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism," to be published in IEEE Transactions, vol. 9, no. 2.

[8] E. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R.Biddle, "Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords," Proc. Ann. Computer Security Applications Conf. (ACSAC), 2010.

[9] Davis, D. Monrose, F. and Reiter, M.K. "On user choice in graphical password schemes". In *Thirteenth Usenix Security Symposium* (San Diego, CA, USA, Aug. 9-13, 2004).

[10] Hossein Nejati, Ngai-man Cheung, Ricardo Sosa and Dawn C.I.Koh. Deep"Captcha: An Image CAPTCHA Based on Depth Perception". ACM digital Library, March 2014.