Graphical Password Authentication using Combination of Advance Cued Click Point and Passpoint Mechanism

Ms. Gurvinder Kaur
Assosiated Professor, Department CSE, Chandigarh University, Chandigarh, India

Abstract: The major quandary of user registration, mostly text base password, is prominent. In the authenticate user be inclined to cull simple passwords which is frequently in mind that are straightforward for assailers to conjecture, arduous machine engendered password mostly perplexed to user take in mind. User authentication password using combination of cued click points and Pass Points scheme of graphical password which showsease of use and security assessments. This paper incorporates the influence to secure user authentication and graphical password utilizing cued click-points and pass points so that users cull more arbitrary or more arduous to conjecture the passwords. In click-based graphical passwords, image or video frame that provide database to load the image, and then store all information into database. Mainly passwords are composed of strings which have letters as well as digits.

Keywords - Cued Click Point, Graphical Password Authentication.

I. INTRODUCTION

User authentication is an essential part in most PC security setting. There are three noteworthy zones where human computer collaboration is vital: authentication, security operations, and developing secure systems. A key territory in security examination is authentication, the determination of whether a user ought to be permitted access to a given framework or resources. The most widely recognized computer authentication strategy is for a user to present a user name and a text password. A password is a mystery word or series of characters that is utilized for authentication, to demonstrate personality on the other hand access a resource. The password ought to be kept secret from those not permitted access. It is the obligation of the individual to keep the password secure. But, humans tend to choose passwords which are easy to guess. The vulnerabilities of this system have been well known. One of the principle issues is the trouble of recollecting passwords. To address the issues with conventional username password authentication, other verification strategies like biometrics and graphical passwords can be used.

Graphical password schemes have been proposed as a conceivable different option for text based plans, propelled halfway by the way that people can recollect pictures superior to anything content. Pictures are for the most part simpler to be recalled or perceived than content. In expansion, if the quantity of conceivable pictures is adequately extensive, the possible password space of a graphical password scheme may exceed that of text based scheme and in this manner probably offer better imperviousness to word reference assaults. In view of these (assumed) points of interest, there is a developing enthusiasm for graphical password In addition to workstation and web log-in applications, graphical passwords have also been applied to ATM machines and mobile devices.

A graphical password is an authentication system that works by having the user select from images, in a particular order, presented in a graphical interface (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA). A graphical password is easier than a text-based password for most people to remember. Pictures are generally easier to be remembered than text. If the number of pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text based schemes and hence may prove to offer better resistance to dictionary attacks.

II. LITERATURE REVIEW

It seeks to describe, summarize, evaluate, clarify and integrate the content of primary reports in graphical authentication.

Varenhorst (1991) proposed a graphical authentication algorithm called passdoodle algorithm. A Passdoddle Graphical Authentication algorithm which used the idea of hand written designs or words, drawn with a pen onto a sensitive touchable screen was proposed in 2004 by Goldberg and his college. They confirmed that users were able to remember complete doodle images as they would with textual passwords [20].

Jermyn Ian et al. (1991) designed the draw secret algorithm. This method consisted of an interface that had a rectangular grid of size G *G, which allowed the user to draw a simple picture on a 2D grid. Each cell in this grid is earmarked by discrete rectangular coordinates (x,y). The stroke should be a sequence of cells which does not contain a pen up event. Hence the password is defined as some strokes, separated by the pen up event. At the time of authentication, the user needs to re-draw the picture by creating the stroke in exactly the same order as in the registration phase. If the drawing hits the exact grids in the same order, the user is authenticated [1].

Thorpe &Oorschot (2004) described Grid selection algorithm increases the DAS password space. This research was conducted on the complexity of the DAS technique based on password length and stroke count by Thorpe and Orschot. Their study showedthat the item which has the greatest effect on the DAS password space is the number of strokes. This means that for a fixed password length, if a few strokes are selected then the password space will significantly decrease. To enhance security, Thorpe and Orschot created a “Grid Selection” technique. The selection grid has a large rectangular region to zoom in on, from the grid which the user selects their key for their password. This definitely increases the DAS password space [7].

Di Lin et al. (2007) stated the QDAS method as a boost to the DAS method, by encoding each stroke. The raw encoding consists of its starting cell and the order of qualitative direction change in the stroke vis-a-vie the grid. A directional change is when the pen passes over a cell boundary to the direction of the pass in the previous cell boundary. Research has shown that the image which has a hot spot is pivotal as a background image. Albeit this model applies dynamic grid transformation to mask the process of creating the password, this method could be safer than the original DAS in the fight against shoulder surfing attack and further it has greater entropy than the previous DAS [2].

Syukri et al. (1998) proposed a system where authentication is kicked in when the users draw their signatures utilizing the mouse. This technique has a two step process, registration and verification. During the registration stage, the user will be required to draw his signature with the mouse, whereupon the system will extract the signature area and either enlarge or scale-down the signatures, rotating the same if necessary (Alternatively known as normalizing). The information will later be stored in the database. The verification stage initially receives the user input, where upon the normalization takes place, and then extracts the parameters of the signature. By using a dynamic updateable database and the geometric average means, verification will be performed [8].

Blonder (1966) presented a method where in a pre-determined image is presented to the user on a visual display so that the user should be able point to one or more predetermined positions on the image (tap regions) in a predetermined order as a way of pointing out his or her authorization to access the resource. Blonder maintained that the method was secure according to the millions of different regions [3].

Wiedenbeck et al. (2005) designed the PassPoint algorithm in order to cover the image limitations of the Blonder Algorithm. The picture could be any natural picture or painting but at the same time had to be rich enough in order for it to have many possible click points. On the other hand the existence of the image has no role other than helping the user to remember the click point. This algorithm has another flexibility which makes it possible for there to be no need for artificial pictures which have pre-selected regions to be clicked like The Blonder algorithm. During the registration phase the user chooses several points on the picture in a certain sequence. To log in, the user only needs to click close to the chosen click points, and inside some adjustable tolerable distance, say within 0.25 cm from the actual click point. The Passpoint system has enough features for creating a high entropy algorithm. Since any pixel in the image is a candidate for a click point thus there are hundreds of possible memorable points in the challenge image [4].

Duaphi (2007) designed the Background DAS Algorithm (BDAS), this method added a background image to the original DAS, such that both the background image and the drawing grid is the key to cued recall. The user begins by trying to have a secret in mind which is made up of three points from different categories. Firstly the user starts to draw using the point from a background image. Then the next point of user is that the user’s choice of the secret is affected by various characteristics of the image. The last alternative for the user is a mix of the two previous methods [4,5].

Vamponski, (2006) proposed Passmap algorithm that shows a sample of a PassMap password for a passenger who wants to take a trip to Europe as follows: One day a tour in Paris around the Eiffel then a tour in London around Big Ben. After these two tours, the third tour will be in Moscow. The passenger must be able to visit all of them in a map. Referring to the Figure below, it will be easy to memorize the trip in a map [3].

Passlogic Inc. Co., (2002) concluded the Passlogix algorithm. Their scheme, Passlogix v-Go, utilizes a technique known as "Repeating a sequence of actions" meaning creating a password in a chronological sequence. Users select their background images based on the environment, for example in the kitchen, bathroom, bedroom or others. User can click on a series of items in the image as password. For example in the kitchen environment a user can prepare a meal by selecting a fast food from the refrigerator and put on the hot plate, select some vegetables and wash them, then put them on the launch desk. In case another environment such as the cocktail lounge is used, this will allow users to select their favorite vodka, brandy or whiskey and mix it with other cocktails. This type of authentication is easy to remember and fun to use [6].

SFR Company (2003) discovered VisKey algorithm, is a one of the recall based authentication schemes commercialized by SFR Company in Germany which was created specifically for mobile devices such as PDAs. To form a password, all users need to do is to tap their spots in sequence. Weaknesses: Input tolerance is the major drawback of this method. This algorithm permits all input within a certain tolerance area around it, since it is difficult to point to the exact spots on the picture. The size of this area can be pre-defined by users. A certain degree of precaution, related to the input precision, needs to be exercised, as there is a straight forward correlation between the security and the usability of the password. Practically, the setting of parameters with a four spot VisKey theoretically offers almost 1 billion possibilities to define a password. However, such is not large enough to avoid the off-line attacks by a high-speed computer. A minimum of seven defined spots are needed in order to overcome the brute force attacks [7].

Brostoff&Sasse (2000) developed the Passface Algorithm which gives the idea to choose a face of humans as a password. Firstly, a trial session starts with the user in order to have an adventure for the real login process. During the registration phase the user chooses whether their image password should be a male or female picture, then chooses four faces from decoy images as the future password. During the login phase, a grid which contains nine pictures is shown to the user. Only one of the user's passwords among four is shown to user in this grid, and the other eight pictures are decoys which are selected from the bank of pictures. Because the password of user contains four faces so the grid repeats continually for four times and each repetition contains one of the password pictures. If one of the passwords has been shown in one grid, it will not be shown in the next grid. On the other hand the password faces are randomly placed in grids which help to create a more secure environment for the user against shoulder-surfing and packet sniffing attacks. The user tries to identify his four passwords among the other pictures twice in a row. According to research, this is one of the algorithms which cover the most of the usability features like ease of use, and straightforward creation and recognition [6].

GENERALIZATION OF RESULTS:

The following issues have been covered in the above study:

- A lot of work has been done in the field of user password for authentication. The Researcher has discovered various methods for graphical password authentication using various ways of authentication.
- The Researchers reviewed existing graphical password schemes by cataloguing them according to several usability and security characteristics. Little consistency in the types of evaluations conducted on graphical passwords, with most evaluations focusing on either usability or security but not both.

The following issues are still uncovered:

- Above works focus on the security and usability of an algorithm, but not both.
- Most of existing graphical password schemes are vulnerable to shoulder-surfing attacks.

Any person can click the picture of graphical images and hack the password easily. But the proposed algorithm will provide security from shoulder-surfing.

PROBLEM STATEMENT:

Present problem is entitled as "Design of an Algorithm on graphical password authentication". The present study is conducted to design a new click-based graphical password scheme called Advance Cued Click Points (ACCP), removed the problems of text based algorithm and enhance the security of the system. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point at which point they can cancel their attempt and retry from the beginning. It also makes attacks based on hotspot analysis more challenging.

III. PROPOSED METHODOLOGY

To enhance the security of the PassPoint algorithm, here present the new algorithm that is based on click cued point and pass point for secure authentication. In this algorithm, uses five images rather than single image as used in PassPoint. Here guessing point combinations are also increased which increases the security.

REGISTRATION INTERFACE:

Fig 3.1 shows the registration interface, here user firstly enrolls and read the values in the database. At that point the number of these values is coordinated with the aggregate number of values(12). On the off chance that the values are 12 then the client enters in the first period of password creation and chooses first picture from database. After determination of picture, the client is clicked five focuses on a picture. In the event that five focuses are clicked accurately then the client chooses haphazardly five pictures from regis database and clicks a point on each picture. After five pictures choice, the user is entered in last stage. In last stage, the user again chooses a picture from database regis and select five pixel focuses on a picture. At that point every one of the pixels will be put away in the database. Toward the end, the user is enlisted appropriately and the user will be effortlessly login to system through same password.

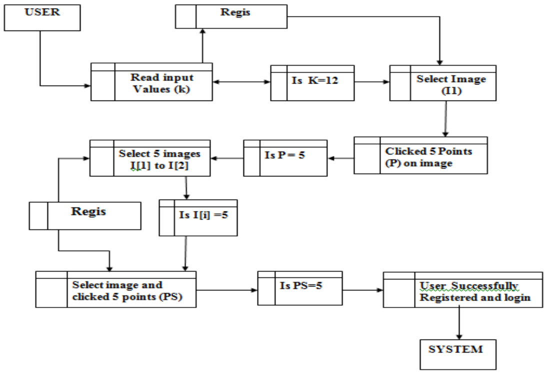

USER
Regis
Read input Values (k)
Is K=12
Select Image (I1)
Clicked 5 Points (P) on image
Is P= 5
Select 5 images I[1] to I[2]
Regis
Is I[i] =5
Select image and clicked 5 points (PS)
Is PS=5
User Successfully Registered and login
SYSTEM

Fig. 3.1 Registration interface for graphical password authentication

LOGIN PHASE:

Fig 3.2 shows the login interface; here firstly user enters the username and password. Then the password matched with already password, if the password matches to already password then the user enters in the first phase of graphical password authentication. In first phase, user selects an image from given images and taps on five points on an image. When the clicked points are coordinated to already stored points, then the user will enter in the second phase for further authentication. In second phase, the user selects five images rather than to select a single image. Selected images are matched to already images then the user will be entered in third phase. In third phase, again user selects an image from given images and will click on five points on an image. Then pixel points will matches to already pixels. When these pixels are matched, then the user will be authenticated to use the system.

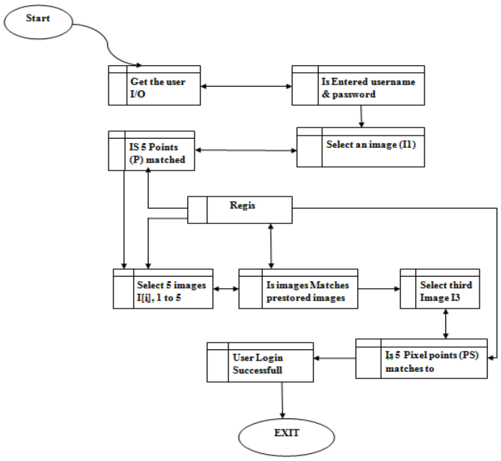
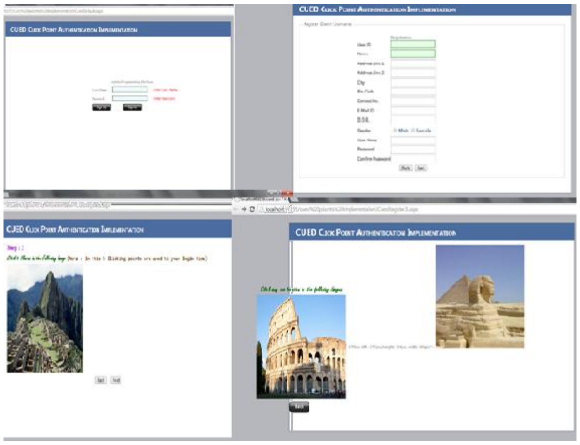

Start
Get the user I/O
Is Entered username & password
Select an image (I1)
IS 5 Points (P) matched
Regis
Select 5 images I[i], 1 to 5
Is images Matches prestored images
Select third Image I3
Is 5 Pixel points (PS) matches to
User Login Successfull
EXIT

Fig. 3.2 Login interface for graphical password authentication

Fig 3.2 shows the login interface;here firstly user enters the username and password. Then the password matched with already password, if the password matches to already password then the user enters in the first phase of graphical password authentication. In first phase, user selects an image from given images and taps on five points on an image. When the clicked points are coordinated to already stored points, then the user will enter in the second phase for further authentication. In second phase, the user selects five images rather than to select a single image.


CUED Click Point Authentication Implementation

CUED Click Point Authentication Implementation

CUED Click Point Authentication Implementation

CUED Click Point Authentication Implementation

Fig. 3.3 Login Interface

Selected images are matched to already images then the user will be entered in third phase. In third phase, again user selects an image from given images and will click on five points on an image. Then pixel points will matches to already pixels. When these pixels are matched, then the user will be authenticated to use the system.

Fig 3.3 Shows the login interface, in which firstly find out whether the user is new or already registered. If a user is already registered then user fills the User Name and the password in the site and enters in login phase by clicking on sign up. But if the user is new user then user clicks on Sign In hyperlink and then user enters in registration interface.

This section collects all text based information of the user and stores that information in database for further detail. When the user completes this information properly then the user navigates to next three graphical phases that are the part of registration. In First phase, there will be user clicks on the five points on the chosen image. Firstly image is to be chosen from different images and then click on different five points on that image. Then the user will click on next button and navigate to next stage of graphical password. In second phase user chooses five images simultaneously one by one. On each and every image user clicks one point and goes on further image. After click on five images user clicks on submit button and then on the next button. Then the user navigates to next phase of graphical password creation.

In last phase again user clicks on five points of an image. Here pixel scheme is used for click a point that will be stored in database. After flapping on five points the user clicked on submit button and navigates to login phase. Here the user creates their own graphical password and can be authenticated in system through this password.

IV. RESULTS

At the time of login, the sequence of images is given to the user which was saved one by one at the time of the registration. Now the user selects the region with the gesture that was used at the time of registration. For every image, the algorithm calculates the parameter’s and matches with the previously stored parameters for that image with some tolerance value. If the match is a success then next image is fetched from the database and the process is repeated and if the match is unsuccessful then the user is not notified until the end and at the next sequence a random image is given to the user and login fail flag is activated. This approach increases the total search space of the attacker and also smart users can select complex regions.

Number of Images	6
Size of Image	300 * 300
Size of Grid	100 * 70
Size of Grid Cells	3 * 3
Number of images for authentication	8
Total attempts	10

Table 4.1 Image configuration

Above given Table 4.1 shows the description of images used to create graphical password or authenticate a system.

V. CONCLUSION

This work focused on the usability of Clicked Cued Points and pass point, but its security is also an important issue. Clicked Cued Points seems to hold out the prospect of a much more secure system. It is easy to obtain large passwords spaces. Furthermore, in this experiment it appears that users rarely chose points that were within the tolerance around the click point of another participant. Finally, there is currently no efficient way of creating dictionary attacks against the system. These observations point to further study of the security and usability of both Clicked Cued Points and Pass Point.

In this algorithm, initially checks that the user is new or already registered. If the user is new then the user enters in the registration phase. In Registration phase, firstly input is taken from the user. After completion of all the information, the user will navigate to first phase of graphical password authentication. In first phase, the user will select an image and click five points on an image. When the user has selected five points then these points will be stored in database and the user will navigate to second stage. At this stage click cued point algorithm will be applied to create the password, the user will select different five images and click single point on every image. When the second stage is completed then the images and clicked points stores in the database, the user will enter in the third stage of the graphical password creation. In the third stage, the user again will select an image and now clicks five pixel points on an image. After third stage completion, these five pixel point’s position will be stored in database and the user will be able to log in for the system use.

During password creation, a discretization method is used to determine a click-point’s tolerance square and its corresponding grid. For each click-point in a Subsequent login attempt, this grid is retrieved and used to determine whether the click-point falls within tolerance of the original point. Each point that the mouse has clicked will be saved into database for future use. The mouse click will continue being recorded up to specific click point and the data will append to the database.

Second phase of graphical password authentication is login phase. In this phase, system firstly checks the user password and username. When the user is already registered, the user can login for system. Entered username and password are matched with already stored passwords, when password will be correct then user will enters in first stage of password authentication. Here the user selects same image and same five points as already stored in database. If these points match the already stored points in the database, the user will select five images of second stage. When these five images and five clicked points match to already stored images and points, then the user will be redirected to last stage. The user will choose an image in last stage and click five points. When these clicked pixels are matched correctly with already stored pixels, then the user will authenticate for the system.

VI. FUTURE SCOPES

Future work should include a thorough assessment of the viability of ACCP as an authentication mechanism, including a long term study of how these passwords work in practice for general websites and whether longer ACCP passwords would be usable. The security of ACCP also deserves closer examination, and should address how attackers might exploit the emergence of hotspots. To improve the security of the system is the future work will consider the multi-factor authentication techniques. Multi-factor technique may combine the graphical password and visual-cryptography.

REFERENCES

[1] Jermyn Ian, A. Mayer, F. Monrose, M. K. Reiter, A. D. Rubin; “The design and analysis of graphical passwords”, Proceedings of the Eighth USENIX Security Symposium, USENIX Association 1–14, 1999.

[2] Di Lin, Paul Dunphy, Patrick Olivier, Jeff Yan; “Graphical Passwords and Qualitative Spatial Relations”, Proceedings of the 3rd Symposium on Usable privacy and security, Pennsylvania, ACM,2007.

[3] Greg E. Blonder; “Graphical Password”, U.S. Patent No. 5559961,1996.

[4] Susan Wiedenbeck, Jean-Camille Birget, Alex Brodskiy;”Authentication Using Graphical Passwords:Effects of Tolerance and Image Choice”, Symposium On Usable Privacy and Security (SOUPS), Pittsburgh, PA, USA 2005b.

[5] Roman V. Yampolskiy; “User Authentication via Behavior Based Passwords”; IEEE Explore, 2007.

[6] Paul Dunphy, Jeff Yan; “Do Background Images Improve “Draw a Secret” Graphical Passwords?”, Proceedings of the 14th ACM conference on Computer and communications security. Alexandria, Virginia, USA, 2007.

[7] J. Thorpe and P. C. v. Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords," in Proceedings of the 20th Annual Computer Security Applications Conference. Tucson, Arizona, 2004.

[8] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer-Verlag Lecture Notes in Computer Science (1438), pp. 403-441,1998.