DESIGN, IMPLEMENTATION AND EVALUATION OF A KNOWLEDGE BASED AUTHENTICATION SCHEME UPON COMPELLING PLAIT CLICKS

Chalichima Harshitha [1], Devika Rani [2]

[1]Pursuing M.tech (CSE) , [2]Assistant professor (CSE) ,
Nalanda Institute of Engineering & Technology, Siddharta Nagar,
Kantepudi (v), Sattenapalli, Guntur, Andhra Pradesh, India – 522483

IJARSE

ABSTRACT

In Digital technology authentication is very important. Different graphical password schemes have been derived as alternatives to text based passwords. We have different methods those uses special symbols and alphanumeric characters to create passwords. But using of these methods there is a possibility of hacking the passwords easily by attackers and third parties. And remembering those passwords consisting of symbols and special characters is very difficult. By using text based passwords we have some usability and security problems. To resolving these problems so many techniques are suggested for providing authentication and revealing graphical password methods so that to reduce the cost and usage. Graphical passwords are created by using images and it has some disadvantages such as shoulder surfing problem and hotspot problem. To reduce the above problems Sonia chiasson et al proposed persuasive cued click-point based method with cued based graphical password technique. In this paper we proposed evaluation of the persuasive cued click points (CCP) graphical password method. This includes usability and security evaluations and implementation issues. The Main aim of this knowledge based authentication system is to provide users in selecting passwords with high security. Users can able to create and re-enters their passwords. In this method users click on one point on each image instead of clicking on different points on one image. User selects one click point on each image so that the sequence of click points on next images is depended on previous click point. By this technique user uses cued click point as gate pass, saying that choosing and remembering only one point per image was very easy and here each image is referred with corresponding click point where it is located. We use to influence user choice in click based graphical passwords and motivate users to select more random and so that it is more difficult to guess the user selected click points. The main advantage of cued click point is that producing implicit feedback immediately says that the correct user whether their latest click point was correctly entered.

***Index Terms*: Graphical Passwords, Authentication, Click Points, Privacy, Password Protection, Guessing Attacks.**

I INTRODUCTION

Authentication is an important issue, which prevents unauthorized person in a computer based information security environment system. In Present days, most frequently used technique in the information security computer based system for authentication is text based authentication. In this technique user create passwords with the help of characters, special symbols, numbers, keywords and special characters and problems of knowledge based authentication is text based passwords. Sometimes user can create memorable passwords that they are easily guessed by hackers where as a strong system which generate complicate passwords are difficult for users to remember. But a password authentication system should provide strong passwords as well as maintain memorability. The previous results that text based passwords systems have struggled with security and usability issues. As a solution for these problems graphical passwords techniques have been introduced. The graphical passwords based authentication is using images instead of text to creating user password.

Graphical passwords can be divided into 3 types: Draw-based, choice based and click-based. ***Draw based graphical password*** method users have to draw some secrete. Where as in ***Choice-based type*** users have flexibility to select sequence of images to set the password. And ***click-based method*** a user has to select click points on the image. The present technique follows authentication techniques like pass points, cued click points and persuasive cued click points. In ***Pass Point Method*** method the users have to select click points on a single image and in ***Cued Click Point Method*** users can select click points up to n level of images that means in each level it takes a single click point on a single image. And where in the case of ***Persuasive Cued Click Points*** it selects one click point on one image using persuasive technology. When we consider the security issues, the click based graphical authentication having problem with hotspot and shoulder surfing problems. To solve these issues, the following solutions are made in this paper:

- ➢ For eliminate hotspot problem we uses persuasive technology. In this system activates some area for selecting the click point on the image and further user doesn't have the rights to change that selected area.
- ➢ To reduce shoulder surfing problem, it uses double click method for selecting the click points and single click method for storing empty values in the login phase. Even though an attacker got information about click points it's hard to break our password. Because the user applies either single or double click methods randomly to confuse attacker.

We are proposing the authentication systems allow user choice when it is required to users to create or to provide stronger passwords. In the current system users may selects weak passwords those are easy for attackers to predict or hacking. Hence it is more necessity, to discouraging users from making such simple and easy password choices. In this paper we proposed a consistent assimilation of earlier work. The systematic examination provides a comprehensive and integrated evaluation of Persuasive Cued Click Points covering both usability and security issues for advance understanding as is prudent before practical deployment of new security mechanisms. Results show that cued click points is effective at reducing hotspots which are the areas of the image where users are more likely to select click points and avoiding patterns formed by click points within a password when still maintaining usability.

IJARSE

II RELATED WORK

Recently the security problem has been formulated as a technical problem having some security and usability problems while we are using text passwords as user authentication methods. The security researchers has evolved hastily in response to security threats on the one hand increasing attention in practice and on the other hand motivating research innovation. Here security problems are defined as attacks like an intruder looking for one's shoulder to get information is also called as shoulder surfing etc and having limited password space is known as usability problem. Some researchers provide technology alternatives for text based passwords as biometric systems and they have their own drawbacks. So to overcome from these drawbacks, graphical passwords had been introduced by Greg Blonder in 1996 which offers a solution as another alternative as the passwords which we are focusing are cued recall click based graphical passwords also called as locimetric.

Graphical passwords consist of clicking on images rather than typing alphanumeric strings may help to conquer the problem of creating secure and memorable passwords. The graphical password method using click point provides the alternative for the text password cued click points are used to increase the memeorablity of the user that it is fully knowledge based authentication. The usability and security issues associated with alphanumeric passwords as the password problem. This arises because passwords are expected to comply with two conflicting requirements,

- Passwords must be easier to remember and the user authentication protocol should be executable quickly and easily by humans.
- Passwords should be secured that is they should be random and should be hard to find or to guess.
- Passwords are changed frequently.
- Passwords should be different on different accounts of the same user.
- Passwords could not be written down on anywhere or stored in plain text.
- Passwords problem arises primarily from fundamental limitations of human long term memory (LTM).Once a password has been chosen and learned the user must be able to recall it to login. Though people regularly forget their passwords.

To eliminating these problems with text based password authentication, Graphical password authentication techniques and algorithms are introduced. S. Wiedenbeck et al. in 2005 introduces a pass points (PP) technique to achieve usability by reducing the problem of memorable passwords over text based passwords method. And Sonia Chiasson et al. proposed one method called cued click points (CCP) which provides more usability and security than pass-points method.

2.1 Pass Points (PP)

In Pass Points Technique user selects N random points in an image presented to user. In this system an image is selected from set of images present in a gallery and user is shown the image. The job of user is to click N points as shown in Fig.1.When the user clicks on the point's features from points are stored and not the point itself. Since storing points directly reduces the security of the technique. Because it is very difficult to remember the random points user chooses to select points on images that can be easily recognized in the image. This is called as Hot Spot.

IJARSE

This system is having advantage as simplicity of implementation but it has one drawback that is low security. In another alternative of this system is the user himself picks the image, it will increases the security of the graphical password. Although the user has to always enter the same image and within some system defined lenience place on the image for each click point during authentication which means that image must be physically present in the client system.

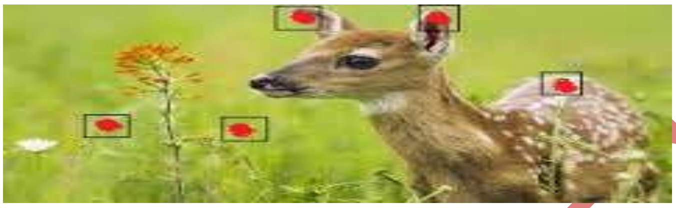

Fig.1. Pass Points (PP)

2.2 Cued Click-Point (CCP)

In cued click point (CCP) is a method which provides more usability and security than pass-points method. In this the user selects one point in each of N images presented to user randomly that means user can select one click point for one image up to N levels. For increasing the security loopholes mentioned in the pass points system distribution of password scheme is developed. In that user is presented with N random different images and user has to click one point at every image. Depending on selected click point of current image next image is displayed randomly by the system as shown in Fig.2.

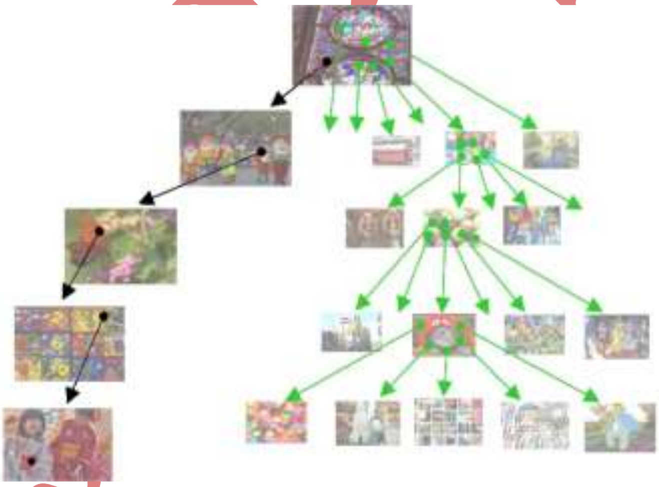

Fig 2. Cued Click Points (CCP) – Here each click determines the next image.

This was explained with an example like that in login phase user should follow the order of selection of click points within the acceptance area. During login phase, the image is visible as blurred image except for a small focus area. Instead of using a mouse to select their click points the user enter Y-for ‘yes’ or N-for ‘no’ on the keyboard. In other way user use the right and left mouse buttons to indicate if their click point is within the focused area. This process repeats for some rounds until all N click points are identified. An algorithm called centered discretization proposed by Robert Biddle, for calculating tolerance area of click points. Because in graphical passwords computing the tolerance area is essential thing for examining whether user click points are valid or not. So that it removes the problems like false accept and false reject.

IJARSE

The major complexity of this cued click points technique is high as user not only has to remember the images in proper order but also has to remember points in every image. By this method consequently great challenge for the user is to remember the password. In this technique user he selects the number of images and number of points in every image.

III PERSUASIVE CUED CLICK POINTS

Image Based Passwords can be made for providing more security to the passwords rather than text based passwords by increasing the randomness. Increase in randomness increases the complexity of remembering the passwords. So the methods are needed that can provide high security and low predictability at the same time they makes it easy for the users to remember the password click points. In the graphical based authentication hotspots and shoulder surfing problem was reduces the security of click-based graphical passwords because attackers can use skewed password distributions to predict and prioritize higher probability passwords for more successful guessing attacks. Visual attention research shows that different people are attracted to the same predictable areas on an image.

The proposed persuasive cued click points system provides the solutions.

➢ In that the first is to select a random image from database. After that one random block of the image is selected as viewport and rest of the image is blurred. So that the viewport can be shuffled to desired position as per user choice. Then user just has to remember the image and the viewport point as shown in Fig.3.

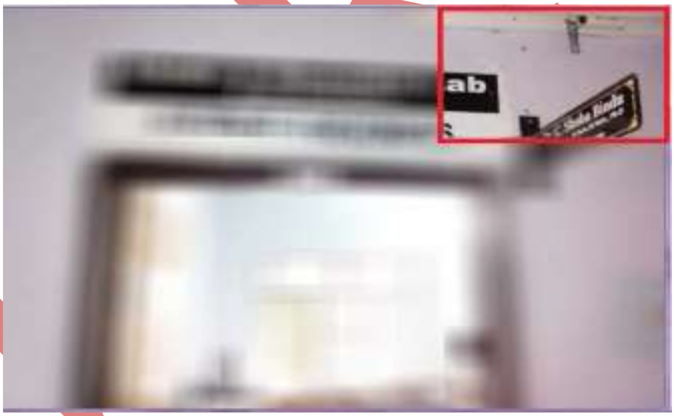

Fig.3. Simple PCCP - The viewport highlights part of the image.

➢ When the user selects a point in the viewport then viewport features are extracted. So that features are based upon color. While checking compare their feature with image features of all images. Then the Closest image in which most of the features are matched is shown next. So that user no needs to remember the next image.

➢ User selects a point then its features are stored and at the same time next matching image is stored.

The Persuasive Cued Click Points System only stores one image for the user and features of click points. The Fig. 4 shows the complete block diagram of PCP graphical password system. So the password is automatically secured as it does not contain any physical location. The user has to specifically remember the first image and the click point. Therefore even though the system makes the password more random it is easy for the user to remember the password. Then the user can select hotspots from second image onwards.

IJARSE

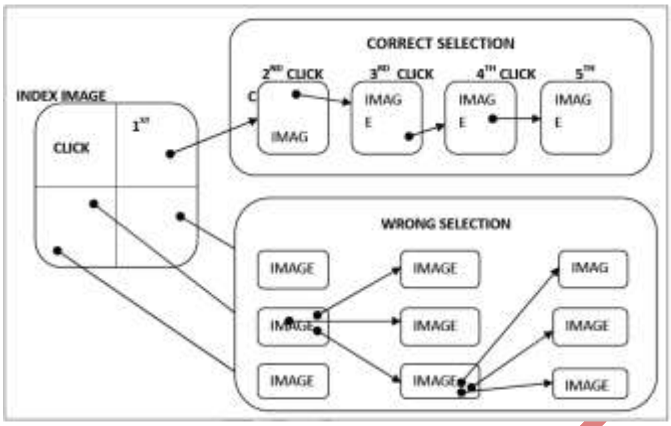

Fig 4 Block diagram of PCP

From an imposter point of view, he has to know the first image, the first click point and then he has to guess all the subsequent click points in subsequent images. A wrong guess alters the image itself thus eliminating the chance of misdetection. As the first view port is purely random and may chances of user clicking on hotspot is minimum. By this proposed system, the drawbacks occurred in existing system that is hotspots can be easily identified and are reduced effectively using hotspot coverage graphs. The Attackers can retrieve the passwords using skewed password distribution. Previous result shows that most of the people are attracted on the same area of the image. Thus it is easy to attack. By the observation it reveals that if users select the click point without any other involvement still there is a chance to appear for hotspot problem. The Researchers suggest that the user choice in all types of graphical passwords is inadvisable. For eliminate this, system involvement is needed to select more random click points while maintaining usability. Then the attackers acquire knowledge of a particular user's credentials through direct observation or through external recording devices such as video cameras while the authorized user enters the information. An attacker who accurately observes one login would have enough information to log in independently, so shoulder surfing is a concern. The PCCP uses persuasive technology to motivate users to select less guessable passwords and make it more difficult to select every click point as hotspot. Mainly at the time of password creation the images are shaded except viewport and it is positioned randomly to avoid hotspots. This hotspot information allows attackers to improve guesses and could have a chance to produce new hotspots. Viewport size is intended to offer a variety of distinct points but still cover only an acceptably small fraction of all possible points. So selection of click point of user must be inside the viewport only. Outside of the viewport will not respond for user clicks. The user has the flexibility to change the view-port area which is provided by the system whenever a user doesn’t satisfy with the generated viewport area. At the login phase, images are displayed without shading and users needed to select correct click points for authentication.

IJARSE

IV CONCLUSION

In password based authentication systems is to maximize the effective password space. This creates the problem on usability when user choice is involved in that. We have shown that it is possible to allow user choice while still increasing the effective password space. Moreover, tools such as PCCP’s viewport cannot be exploited during an attack. The users could be further deterred at some cost in usability issue from selecting obvious click points by limiting the number of shuffles allowed during password creation or by progressively slowing system response in repositioning the viewport with every shuffle past a certain threshold. The major advantage of persuasive cued click point scheme is its large password space since entire image is used for generating the password and it helps in reducing number of hotspots in the image compared to existing click based graphical password systems. So that it provides better security purpose. By this proposed persuasive cued click points design implementation we can achieve the draw backs of present systems like pass points and cued click points approaches.

REFERENCES

[1] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, Paul C. Van Oorschot "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism" on IEEE transactions on dependable and secure computing.

[2] Prof. Anil Kulkarni, Sangameshwar "Design, Implementation and Evaluation of Knowledge-Based Authentication Mechanism Using Persuasive Cued Click-Points" on International Journal of Advanced Research in Computer Science and Software Engineering.

[3] Suresh Pagidala, C. Shoba Bindu "Improved Persuasive Cued Click Points for Knowledge-Based Authentication" on International Journal of Computer Science and Information Technologies.

[4] S. Chiasson, R. Biddle, and P. van Oorschot, "A Second Look at the Usability of Click-Based Graphical Passwords," Proc. ACM Symp. Usable Privacy and Security (SOUPS).

[5] 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.

[6] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security (ESORICS).

AUTHOR PROFILE

Chalichima Harshitha is currently pursuing M.Tech in the Department of Computer Science & Engineering, from Nalanda Institute of Engineering & Technology (NIET), siddharth Nagar, Kantepudi(V), Sattenapalli (M), Guntur (D), Andhra Pradesh , Affiliated to JNTU-KAKINADA.

Devika Rani working as Assistant Professor at Nalanda Institute of Engineering & Technology (NIET), siddharth Nagar, Kantepudi(V), Sattenapalli (M), Guntur (D), Andhra Pradesh , Affiliated to JNTU-KAKINADA.

IJARSE