KNOWLEDGE BASED AUTHENTICATION SYSTEM DESIGN BASED ON PERSUASIVE CUED CLICK POINTS

G Anil Kumar [1], K 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

ABSTRACT

In recent years the usability of information based endorsement system is essential to support users in selecting passwords with top security. By the logic of being from an expanded effective security space. In Digital technology endorsement is very significant. The main aim of this knowledge based authentication system is to afford users in selecting passwords with high protection for digital equipment. Many of the different graphical password schemes have been derived as unconventional to content based passwords. We have different methods those uses special cryptogram and alphanumeric characters to create passwords. But using of these methods there is a prospect of hacking the passwords easily by attackers and third parties. And identification those passwords' consisting of symbols and special characters is very complicated. By using text based passwords we have some usability and sanctuary problems. In this paper we present an incorporated evaluation of the Persuasive Cued Click Points graphical password system for providing authentication and enlightening graphical password methods so that to decrease the cost and usage. It includes usability and security evaluations, and execution considerations. We use persuasion to manipulate user choice in click-based graphical passwords, encouraging users to select extra random, and hence more difficult to estimate, click-points.

Keywords: Cued Clicks Points, Digital Technology, Endorsement, Graphical Passwords, Privacy.

I INTRODUCTION

Text passwords are the most conventional user substantiation method, previous than have security and usability problems. While alternatives such as biometric systems and tokens have their own drawbacks. Graphical passwords propose another alternative. The problems of information based authentication, typically text based passwords, are well known. Users regularly create memorable passwords that are easy for attackers to estimate, but strong system assigned passwords are tough for users to remember. Users can capable to create and re enters their passwords. In this method users click on one point on every image as an choice of clicking on different points on one image. A user selects one click point on each image so that the series of click points on next images is depended on earlier click point. By this process user uses cued click point as gate pass, saying that

choosing and finding 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 control user selection in click based graphical passwords and support users to select more random and so that it is more complicated to guess the user selected click points. The main advantage of cued click point is that producing implicit response immediately says that the correct user whether their latest click point was appropriately entered.

Endorsement is an important concern, which prevents illegal person in a computer based information security system. In Present days, most frequently used method in the information security computer based system for authentication is text based authentication. In this procedure user generate passwords with the help of characters, special symbols, numbers, keywords, special characters and problems of information based authentication is text based passwords. Sometimes user can create unforgettable passwords that they are simply guessed by hackers where as a strong system which generate complicate passwords are complex for users to remember. But password authentication system should provide strong passwords as well as preserve memorability. The earlier results that text based passwords systems have struggled with security and usability issues. As a key for these troubles graphical passwords techniques have been introduced. The graphical passwords based endorsement is using images instead of text to create user password.

Graphical passwords can be separated into three types:

Draw based graphical passwords.
Choice based graphical passwords.
Click based graphical passwords

Draw based graphical password technique users have to draw some secrete. Where as in ***Choice based graphical password*** users have flexibility to pick sequence of images to set the password. And ***Click based graphical password*** is a user has to choose click points on the image. The present technique follows endorsement techniques like pass points, cued click points and persuasive cued click points.

In ***Pass Point Method*** the users have to select click points on a single image.

In ***Cued Click Point Method*** users can select click points up to n level of images that means in every level it takes a distinct click point on a single image.

In the case of ***Persuasive Cued Click Points*** it selects single click point on one image using persuasive cued technology.

When we believe the security issues, the click based graphical authentication having crisis with hotspot and shoulder surfing problems. To solve these problems, the following solutions are made in this paper:

For remove hotspot problem we use persuasive technology. In this system activates some area for selecting the click point on the picture and further user doesn't have the privileges to change that selected area.

To condense shoulder surfing problem, it uses double click technique for selecting the click points and single click technique for storing empty values in the login phase. Even though an attacker got information about click points it's tough to break our password. Because the user applies either single or double click techniques randomly to confuse attacker.

We are proposing the endorsement systems allow user choice when it is necessary to users to create or to provide stronger passwords. In the present system users may selects weak passwords those are simple for attackers to expect or hacking. Hence it is more necessity, to discouraging users from creation such simple and easy password choices. In this paper we proposed a consistent adaptation of earlier work. The systematic examination provides a widespread and integrated assessment of Persuasive Cued Click Points covering both usability and security issues for advance understanding as is careful before practical deployment of new security mechanisms. Outcome show that cued click points is effective at dropping hotspots which are the areas of the image where users are more likely to choose click points and avoiding patterns created by click points within a password when still maintaining usability.

II BACKGROUND WORK

Recently the security crisis has been formulated as a technical problem having some security and usability problems while we are using text based passwords as user endorsement methods. The security researchers has evolved hastily in retort to security threats on the one hand increasing attention in practice and on the other hand encouraging 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 gap is known as usability problem. Some researchers provide knowledge alternatives for text based passwords as biometric systems and they have their own drawbacks. So to overcome these drawbacks, graphical passwords had been introduced by Greg Blonder in 1996 which offers a solution as another option 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 defeat the problem of creating secure and unforgettable passwords. The graphical password technique using click point provides the alternative for the text based 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 difficulty. This arises because passwords are estimated to comply with two conflicting requirements, Passwords must be easier to memorize 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 estimate. Passwords are changed frequently. Passwords should be dissimilar 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 basic limitations of human long term memory. Once a password has been chosen and learned the user must be able to recall it to login. Though people repeatedly forget their passwords.

To eliminate 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 difficulty 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 method user selects N random points in an image existing to user. In this method an image is selected from set of images present in a gallery and user is exposed the image. The work 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 openly 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 predictable in the image. This is called as Hot Spot.

This system is having benefit 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 protection of the graphical password. Although the user has to always enter the same image and within some system definite lenience place on the image for each click point during endorsement 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 safety than pass point's technique. In this the user selects one point in each of N images available to user randomly that means user can select one click point for one image up to N levels. For raising the security loopholes mentioned in the pass points classification allocation of password scheme is developed. In that user is presented with N random dissimilar images and user has to click one point at every image. Depending on selected click point of present image next image is displayed randomly by the system as shown in Fig.2.

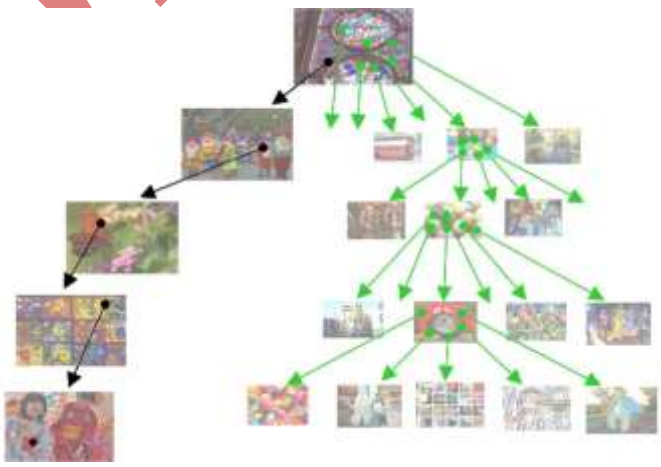

Fig 2. Cued Click Points (CCP) – Here each click determines the next image.

This was explaining with an instance like that in login phase user should pursue the order of set of click points within the acceptance area. During login phase, the image is visible as blurred image except for a small focus area. As an alternative 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 acceptance area is necessary thing for examining whether user click points are valid or not. So that it removes the problems like false accept and false reject.

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 METHOD OF IMPLEMENTATION

3.1 Persuasive Cued Click Points (PCCP)

The image Based Passwords can be made for given that more security to the passwords rather than text based passwords by increasing the unpredictability. Increase in uncertainty 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.

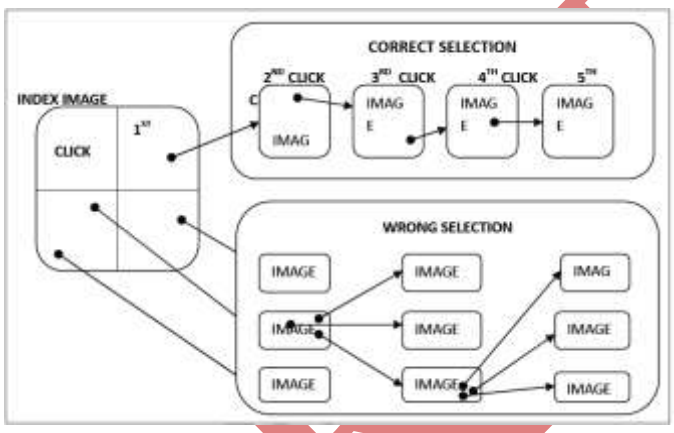

Fig 4 Block diagram of PCCP

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.

IV SUMMARY

A frequent security objective in password based authentication systems is to maximize the efficient password space. This impacts usability when user choice is concerned. We have exposed that it is probable to allow user choice while still raising the effective password space. Also, tools such as PCCP's viewport (used during password creation) cannot be exploited during an attack. Users could be further deterred (at some cost in usability) 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 approaches discussed in this paper present a middle ground between insecure but memorable user-chosen passwords and secure system generated random passwords that are difficult to remember. Providing instructions on creating secure passwords, using password managers, or providing tools such as strength meters for passwords have had only limited success. The problem with such tools is that they require additional effort on the part of users creating passwords and often provide little useful feedback to guide users' actions. In PCCP, creating a less guessable password (by selecting a click-point within the first few system-suggested viewport positions) is the easiest course of action. Users still make a choice but are constrained in their selection.

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

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

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