International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Graphical Password Authentication System Using Persuasive Cued Click Point

Shraddha Wagh[1], Rupali Navalkar[2], Prof.R.P.Bijwe[3]
Final Yr CSE ,H.V.P.M's COET, Amravati

Abstract:- The main issues of knowledge-based authentication usually text-based passwords, are well known. Users tend to choose memorable passwords that are easy for attackers to guess, but strong system assigned passwords are difficult for users to remember. In this paper focuses on the integrated evaluation of the Persuasive Cued Click Points graphical password authentication system, including usability and security. An important usability goal for authentication systems is to support users in selecting better passwords, thus increasing security by expanding the effective password space. In click-based graphical passwords, poorly chosen passwords lead to the emergence of hotspots (portions of the image where users are more likely to select click-points, allowing attackers to mount more successful dictionary attacks). We use persuasion to influence user choice is used in click-based graphical passwords encouraging users to select more random, and hence more difficult to guess, click-points.
Keywords: - Graphical password, authentication, persuasive technology, usable security.

I. INTRODUCTION

There are many things that are 'well know' about passwords; such as that user can't remember strong password and that the passwords they can remember are easy to guess. A password authentication system should encourage strong and less predictable passwords while maintaining memorability and security. This password authentication system allows user choice while influencing users towards stronger passwords. The task of selecting weak passwords (which are easy for attackers to guess) is more tedious, avoids users from making such choices. In effect, this authentication schemes makes choosing a more secure password the path-of-least-resistance. Rather than increasing the burden on users, it is easier to follow the system's suggestions for a secure password - a feature absent in most schemes. We applied this approach to create the first persuasive click-based graphical password system, Persuasive Cued Click- Points (PCCP) and conducted an in lab-lab usability study with 10 participants. Our results show that our Persuasive Cued Click Points scheme is effective at reducing the number of hotspots (areas of the image where users are more likely to select click points) while still maintaining usability. In this paper also analyse the efficiency of tolerance value and security rate.

II. BACKGROUND

Text passwords are the most prevalent user authentication method, but have security and usability problems. Replacements such as biometric systems and tokens have their own drawbacks .Graphical passwords offer another alternative, and are the focus of this paper. Graphical passwords were originally defined by Blonder (1996). In general, graphical passwords techniques are classified into two main categories: recognition-based and recall based graphical techniques. In recognition based ,a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he selected during the registration stage. In recall based graphical password, a user is asked to reproduce something that he created or selected earlier during the registration stage. This paper is based on recall based Technique.

A. Why Graphical Password?

Access to computer systems is most often based on the use of alphanumeric passwords. Though, users have difficulty remembering a password that is long and random-appearing. Instead, they create short, simple, and insecure passwords. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and, therefore, more secure. Using a graphical password, users click on images rather than type alphanumeric characters.

B. Click-Based Graphical Passwords

Graphical password systems are a type of knowledge-based authentication that attempts to leverage the human memory for visual

information. A complete review of graphical passwords is available elsewhere[11]. Of interest herein are cued-recall click-based graphical passwords (also known as locimetric). In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues[13] to aid recall.

Example systems include PassPoints and Cued Click-Points (CCP). In PassPoints, a password consists of a sequence of five click-points on a given image (see Figure 1). Users may select any pixels in the image as click-points for their password. To log in, they repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points. The usability and security of this scheme was evaluated by the original authors and subsequently by others. It was found that although relatively usable, security concerns remain. The primary security problem is hotspots: different users tend to select similar click-points as part of their passwords. Attackers who gain knowledge of these hotspots through harvesting sample passwords or through automated image processing techniques can build attack dictionaries and more successfully guess PassPoints passwords. A dictionary attack consists of using a list of potential passwords (ideally in decreasing order of likelihood) and trying each on the system in turn to see if it leads to a correct login for a given account. Attacks can target a single account, or can try guessing passwords on a large number of accounts in hopes of breaking into any of them.

Fig.1 5 click points on single image

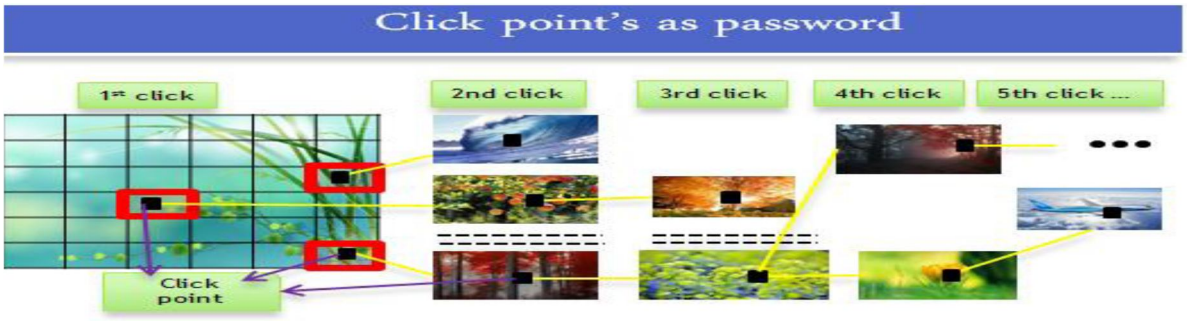

Fig. 2 with CCP, users select one click-point per image. The next image displayed is determined by the current click-point.

C. Persuasive Technology

Persuasive Technology was first articulated by Fogg as using technology to motivate and influence people to behave in a desired manner. Persuasive Technology is the emerging field of "interactive computing systems designed to change people's attitudes and behaviours". An authentication system which applies Persuasive Technology should guide and encourage users to select stronger passwords, but not impose system-generated passwords. To be effective, the users must not ignore the persuasive elements and the resulting passwords must be memorable. As detailed in the next section, our proposed system accomplishes this by making the task of selecting a weak password more tedious and time-consuming. The path-of-least resistance for users is to select a stronger password (not comprised entirely of known hotspots or following a predictable pattern). As a result, the system also has the advantage of minimizing the formation of hotspots across users since click points are more randomly distributed.

III. PERSUASIVE CUED CLICK POINTS

Previous models have shown that hotspots are a problem in click-based graphical passwords, leading to a reduced effective

password space that facilitates more successful dictionary attacks. We investigated whether password choice could be influenced by persuading users to select more random click-points while still maintaining usability. Our goal was to encourage compliance by making the less secure task (i.e., choosing poor or weak passwords) more time-consuming and awkward. In effect, behaving securely became the path-of-least-resistance. Using CCP as a base system, we added a persuasive feature to encourage users to select more secure passwords, and to make it more difficult to select passwords where all five click-points are hotspots.

Fig. 3 PCCP Create Password interface. The viewport highlights part of the image

The theoretical password space for a password system is the total number of. unique passwords that could be generated according to the system specifications.

IV. SYSTEM MODULE

The system designed consist of three modules such as user registration module, picture selection module and system login module. Shown in (fig 4.)

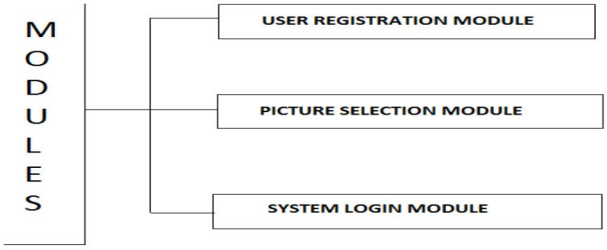

Fig. 4 System design modules.

In user registration module user enter the user name in user name field and also suitable tolerance value (tolerance value is use to compare registration profile vector with login profile vector). When user entered the all registration phase, these user registration data stored in data base and used during login phase for verification. In picture selection phase. there are two ways for selecting picture password authentication.

A. User defines pictures: Pictures are selected by the user from the hard disk or any other image supported devices.
B. System defines pictures: pictures are selected by the user from the database of the password.

V. MODULE INCLUDES

A. User Registration Process

Here enter the username in the username field. Suppose if you are the first time user then you have to register in the new user register button which is provided by the admin the button is also provided for the first time user for the registration of new user and then after the username is stored into the database.

B. Picture Selection Process:

There are two ways for password selection process:

1) User Defined Pictures: Picture's are selected by the user from the Hard Disk or from any other image supported devices for that purpose here we provide button control for selecting the picture and select any one of the image from it

2) System Defined Pictures: Pictures are selected by the user from the database of the password system here also we provide button control for selecting the picture and select any one of the image from it Here user with the username select any one of the point from picture and then that point and the image will be stored into the database

A. User registration flow chart

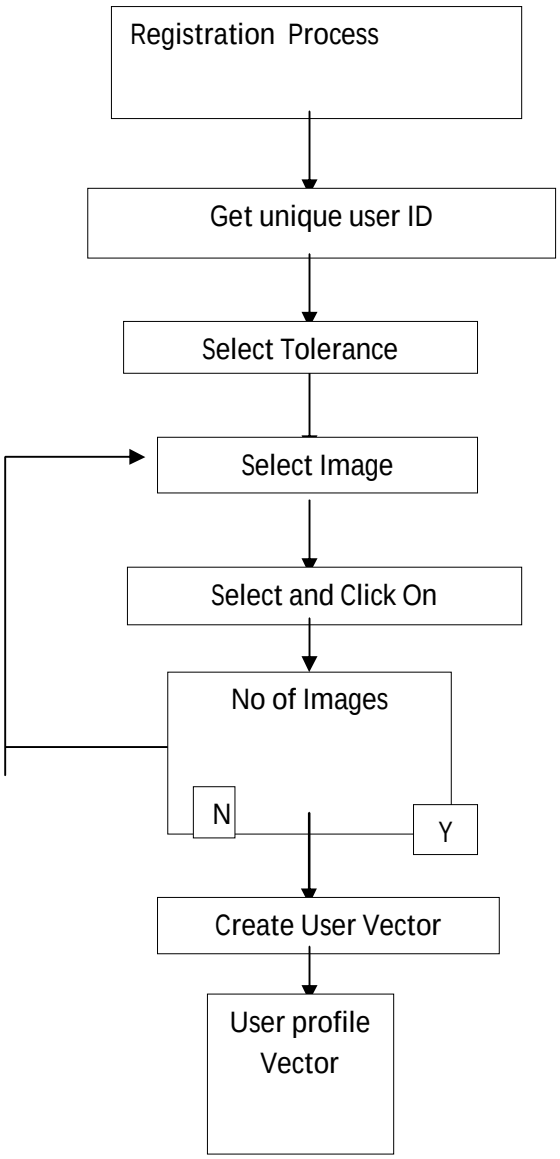

Fig. 5 User registration flowchart

C. Final Registration Process:

It includes both the methods which are describe previously that is user registration process and picture selection process

Step1.user enters the user name here

Step2.Click on the picture button for Select picture for password.

Step 3.Select the point on the picture and click to the next Picture.

Volume 3 Issue III, March 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Step 4. The point on the Last Picture will be calculated as the last point for opening the desired system.
All the points and the picture along with the username will be stored into the database.

D. System Login Process:

1) User Verification Process: User enter the username and then username verification can be done by checking it whether it would be stored in our database or not if yes then it will moves towards further step and if not then it will generate and error message

2) Click point verification process: Verified user can only click on that point which are they selected previously on there respected images and in this whole process the correct click point gives the next image.Last picture in the system will opens the system protected with the password.

B. Login flow chart

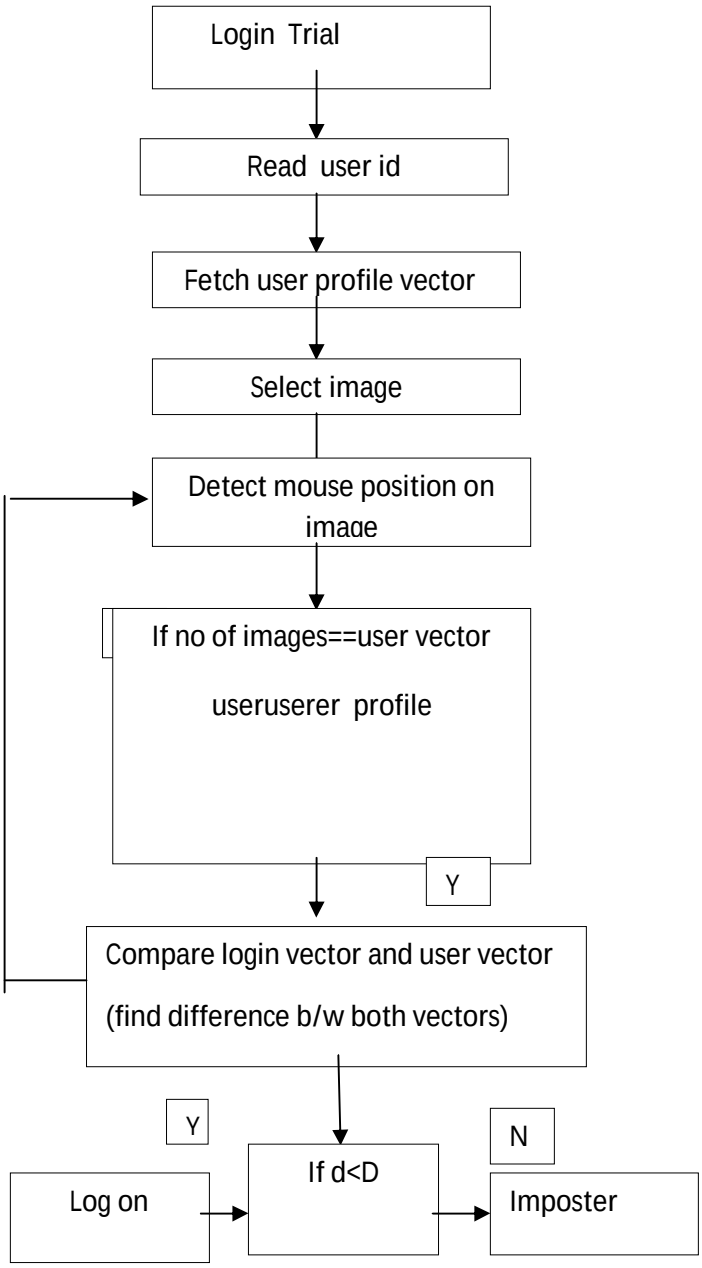

Fig. 6 Login phase flowchart

Above flowchart (see Figure 5) shows the user registration procedure, this procedure include both registration phase (user ID) and picture selection phase. The process flow starts from registering user id and tolerance value. Once user completes all the user details then proceed to next stage, which is selecting click points on generated images, which ranges from 1-5. After done with all these above procedure, user profile vector will be created.

VI. ADVANTAGES

A. Hard disk locking.
B. System log in and log out process.
C. Folder Locking.

VII. CONCLUSION

An important usability and security goal in authentication systems is to help user‟s select better passwords and thus increase the effective password space. We believe that users can be persuaded to select stronger passwords through better user interface design. As an example, we designed Persuasive Cued Click-Points (PCCP) and conducted an usability study to evaluate its effectiveness. We obtained favorable results both for usability and security. PCCP encourages and guides users in selecting more random click-based graphical passwords.

VIII. ACKNOWLEDGEMENT

First of all we would especially like to express sincere gratitude to our parents. It gives us great pleasure and satisfaction in presenting the paper on **“GRAPHICAL PASSWORD AUTHENTICATION SYSTEM USING PERSUASIVE CUED CLICK POINT”** Before we get into the depth of the things, we show our sincere gratitude towards respected teachers, guide, colleagues and all who have directly or indirectly helped us in the completion of this paper successfully

REFERENCES

[1] 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), July 2007.
[2] S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot, “Influencing Users towards Better Passwords: Persuasive Cued Click- Points,” Proc. British HCI Group Ann. Conf. People and Computers: Culture, Creativity, Interaction, Sept. 2008.
[3] A. Forget, E. Stobert, P. van Oorschot, and R. Bddle, “Multiple Password Interference in Text and Click-Based Graphical Passwords,”