Persuasive Cued Click Point (with E-mail and SMS services): Designing and Implementation.

Smruthi Nanukuttan¹, Sruthi Nanukuttan², Pooja. N. Patil³
Guide: Prof. Vikrant. A. Agaskar

¹Department of Computer Engineering, Vidyavardhini college of Engineering and Technology, Mumbai, India.
²,³Department of Computer Engineering, Vidyavardhini college of Engineering and Technology, Mumbai, India.

Abstract: The main problems of authentication, usually text-based passwords, are well known. Users tend to choose more memorable passwords that are easy for attackers to guess, but strong system assigned passwords are difficult for users to remember. The main aim of this paper is on the implementation of the Persuasive Cued Click Points graphical password authentication system, including usability and security. An important factor 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 user select sequence of click points on single image, so attacker can attack the system by randomly selecting the click points. We use persuasion to influence user choice is used in click-based graphical passwords, which helps users to select more random click points, and hence more difficult to guess click-points.

Keywords: Authentication, graphical passwords, usable security, Persuasive cued click points, Advanced Encryption Standard, E-mail, SMS.

1. Introduction

PCCP was designed to reduce patterns and reduce the usefulness of hotspots for attackers. Rather than five click-points sequence on one image, PCCP uses one click-point on five different images shown in sequence. The next image displayed is based on the basis of the previously entered click-point . Creating a password with different click-points results in a different image sequence. The advantage of the pccp is that to attack on the system is not that easy because even though the attacker try the sequence of the clickpoint he is not aware about the registered sequence of images as it won’t give any alert about the wrong sequence of images. Remembering the order of the click-points is no longer a requirement on users, as the system shows the images one at a time. PCCP also provides implicit feedback claimed to be useful only to authorize users. When logging on if the sequence of the click points goes wrong then also the wrong image will get displayed one after another and after the final clickpoint,sms alert will be send to the authorize user(alert: someone is trying to login into your system.). Image security has become a critical issue. So to secure the image password AES algorithm is used in which the click points entered by the user is encrypted and decrypted by using AES algorithm. The following figure 1 shows an Architecture of PCCP

![Figure 1. Architecture of PCCP](image-url)
encrypted and decrypted using AES and then get stored in database.

2. Background

2.1 Text based password

Text based passwords are widely used because they are simple, inexpensive, and convenient mechanisms to use and implement. Text based passwords are the most common form of authentication used to control access of user’s account ranging from the personal identification numbers to users’ accounts like (eg.facebook,gmail). or making the password more complex the user must select alphanumeric, special characters.

At the same time text based passwords are also recognized as being an extremely poor form of protection. These study has been proved that about 80 percent of the security incidents reported to them are related to poorly chosen passwords. It is difficult to handle the text based passwords because a single local computer network may have hundreds or thousands of password-protected accounts and only one needs to be compromised to give an attacker an entry to the local system or network. Now a days there are many hacking tools for text based password through which attacker can easily crack the password that are in text format.

2.2 Graphical based password

To overcome the problem of text based password graphical based password has been introduced. Graphical password systems are a type of knowledge-based authentication that attempts to leverage the human memory for visual information. It has been revealed that human are more intend to remember visuals then the text

In PassPoints, a password consists of a sequence of five click-points on a given image as shown in below figure 2.

Users may select any pixels in the image as click-points for their password. To get into the application, 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.

Although graphical password has been relatively usable, security concerns remain. The primary security problem is hotspots attack that is different users tend to select similar click-points in the image as part of their passwords. Attackers who guess 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 and trying each on the system in turn to see if it leads to a correct login for a given account.

2.3 Persuasive cued click point (Pccp)

To overcome the problem of graphical based problem pccp has been introduced. It inspire users to choose more difficult to guess password, and to make it extra hard to pick passwords as all five clickpoints are in different set of images as shown in figure 3. Specifically, when users created a password, the images were slightly shaded except for a randomly positioned viewport. The viewport’s size was intended to offer a variety of distinct points but still cover only an acceptably small fraction of all possible points. Users were required to select a click-point within this highlighted viewport and could not click outside of this viewport. If they are unable to select a click-point in this region, they could press the “shuffle” button to randomly reposition the viewport. While...
users were allowed to shuffle as often as they wanted. The viewport and shuffle buttons only appeared during password creation.

3. Implementation

In implementation there are three phases i.e
1. Registration phase.
2. Image selection phase.
3. Login phase.

3.1 Registration phase

In the registration phase, as shown in Figure 4, user has to provide user details which has to be unique. After providing the details users has to select set of images which can be user defined or system defined. User selects the level of security by selecting the clickpoints on each images i.e. one clickpoint on one images like this password is generated using sequence of clickpoints in a set of different images. After selecting 5 clickpoints on each image the alert comes that the user registration has been completed successfully. After the successful registration the e-mail is send to the registered users account with the user id.

3.2 Image selection phase

User can select the image using system define or user define. If user goes for system define way to select the image then there is a predefine set of images by default (as shown in proposed algorithm below) user do not require to upload images.

Steps of image selection in system defined:

Step I: User have to provide it’s username to system for system authentication.

Step II: Suppose XYZ username is provided then according to the position of alphabet i.e. (A=1,B=2…z=26) username calculation is done successfully. If sum of XYZ is 75, then system will consider left an side first digit.

Step III: Now 7 is forwarded and set of images from set G is assigned to given username.

Step IV: User should have to select five images from set A and save the clickpoints in that images.

Step V: Finally set of image selected by user i.e. the click points in the images gives the password.
If user is selecting user define way to select set of images then user need to upload a set of images. After selecting the images user has to set clickpoints. For selecting a clickpoint there is viewport. User can manually move the viewport anywhere in the images an select the clickpoint inside the viewport. The coordinates of viewport get stored in the database. For more security the co-ordinates of viewport is stored using the AES algorithm due to which the attacker cannot easily attack the clickpoint which the user has been set.

3.3 Login phase

In the login phase, as shown in Figure 5, user first enters his user id. Then the user is presented with the first image which he had used during registration time in this manner 4 more images will be displayed if the user click wrong clickpoints then also the wrong image will be displayed. While logging, the viewport will not be visible and the user has to click on his registered click-point on the image. If the password matches then the user can enter into the system. If the password entered is wrong then the alert goes as an SMS to the registered users phone number.

![Figure 6/Login phase flowchart.](image)

Conclusion

The main aim is usability and security in authentication systems. It helps user’s to select better passwords and thus increase the effective password space. Graphical authentication scheme is better to remember for the user. We believe that users can be able to select stronger passwords through better user interface design. For the favorable results of usability and security we have designed Persuasive Cued Click-Points (PCCP) and conducted a usability study to evaluate its effectiveness and we had obtained effective results for both usability and security. PCCP encourages users in selecting more random click-based graphical passwords. The approach has proven effective at reducing the hotspots attacks, avoid shoulder surfing problem and also provide high security success rate, while still maintaining usability.

References


