

Account Authentication by Click Point using Image Processing

Rabab Batawala¹, Diksha Umeredkar², Nikita Mahadule³, Priyanka Chikhale⁴, Rashmi Bhoutkar⁵

Department of Computer Science & Engineering, Anjuman College of Engineering & Technology,
Rashtrasant Tukdoji Maharaj University, Nagpur, Maharashtra, India^{1,2,3,4,5}

Abstract: A lot of work has been done in order to secure the login for different applications. These methods range from login ID Password to OTP sending to the user which is very costly due to SMS charges. In this work we are proposing a low cost application that is “Account Authentication by click Points Using Image Processing”. In which user click on an area of image. The next image is based on the previous click-point. Performance was very good in terms of speed, accuracy, and number of errors.

Keywords: Speed, Accuracy, OTP

I. INTRODUCTION

Various graphical password schemes have been proposed as alternatives to text-based passwords. Research and experience have shown that text-based passwords are fraught with both usability and security problems that make them less than desirable solutions. Psychology studies have revealed that the human brain is better at recognizing and recalling images than text graphical passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by images, more secure passwords can be produced and users will not resort to unsafe practices in order to cope.

Authentication is the process of determining whether a user should be allowed to access to a particular system or resource. User can't remember strong password easily and the passwords that can be remembered 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.

In this, we propose a Cued Click Points (CCP) for graphical password authentication. A password consists of one click-point per image for a sequence of images. The next image displayed is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in. CCP offers both improved usability and security.

This application will be helpful in following ways:

- Social media:- This application is used for social media i.e G-mail account, Facebook account, etc.
- Online payment account :- It is used for online payment i.e Google Pay, Paytm, Phone Pay, etc.
- Online banking account :- It is more secure for online banking account.

II. LITERATURE REVIEW

Various graphical password schemes have been proposed at alternatives to text-based passwords. Research has shown that text-based passwords are filled with both usability and security problem that make them less desirable solutions. Studies revealed that the human brain is better at recognizing and recalling images than text.

Considering the applications, the following are based on click points.

- Graphical passwords are meant to capitalize on this human characteristic in hopes that by reducing the memory burden on user, coupled with a larger full password space offered by images, more secure offered by images, more secure password can be produced and user will not resort to unsafe practices in order to cope.
- Graphical passwords may offer better security than text-based password because most of the people, in an attempt to memorize text-based passwords, use plain words (rather than the jumble of characters).

- A dictionary search can hit on a password and allow a hacker to gain entry into a system in seconds. But if a series of selected images is used on successive screen pages, and if there are many images on each page, a hacker must try every possible combination at random

III. PROPOSED SYSTEM

In CCP, users click one point on each 5 images rather than on five points on one image. It offers cued recall with sound signature to assure that the point chosen on image is correct and user must be authorized to use the application or upload or download or they may access the resources and if the chosen points are incorrect then login fails as well as user required to take another login trial means user may get indication of authentication failure only after the final click. It also makes attacks based on hotspot analysis more challenging. To develop a system that is alternative to the text-based or pass-point passwords that offers cued-recall. The system also provides more challenging for attacks based on hotspot analysis. This increases the security by using the sound signature. Proposed system which → Increase the remembrance of password. → Provide more security. → Provide high reliability system. → System is secure and user friendly

This application includes the following five modules:

Module 1: Registration Page

This is the Registration Page which in which user has to register before login.

Module 2: Login Page

This is the login Page which User have to login by entering name and correct password

Module 3: Front view page

This is the Front view of our application which shows animated image.

Module 4: image shuffling

This is the Format of Click Point which have the description of our Web application

Module 5: Selected Shuffled Block Screen

This module will provide the Selected Shuffled Block Screen in which we will click on the click points.

IV. AIMS AND OBJECTIVES

The main purpose of “Account Authentication By Click Point Using Image Processing” system is to provide a way for security.

The goals of the system are:

- To provide no need to remember password.
- Key point's detection is difficult for hackers.
- To provide easy way to use.
- This is highly secured of the system.
- It is easy to remember the image but difficult to crack.

V. CONCLUSION

The proposed Cued Click Points scheme shows promise as a usable and memorable authentication mechanism. By taking advantage of users ability to recognize images and the memory trigger associated with seeing a new image, with the sound signature chosen by them CCP has advantages over Pass Points in terms of usability. Being cued as each images shown and having to remember only one click-point per image appears easier than having to remember an ordered series of clicks on one image. CCP offers a more secure alternative to Pass Points. CCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then conduct hotspot analysis on each of these images.

VI. REFERENCES

- [1]. Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, P. C. van Oorschot, "Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism", IEEE Trans, Vol 9, Issue 2.
- [2]. S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using Cued Click Points," in European Symposium on Research in Computer Security (ESORICS), LNCS 4734, September 2007.
- [3]. Jain, A. Ross, & S. Pankanti, "Biometrics: a tool for information security," Transactions on information forensics & Security (TIFS), vol.1, no.2
- [4]. D. Nelson, V. Reed, & J. Walling, "Pictorial Superiority Effect," Journal of Experimental Psychology: Human Learning & Memory, vol. 2, no.5. ISSN: 2278-1684 Volume2, July-August 2012, PP 25-45
- [5]. M. S. Sukeshini Jadhav, "Electronic Waste: A Growing Concern in Today's Environment Sustainability", International Journal of Social Science and Inter-Disciplinary Research, ISSN: 2277-3630 Volume2, February 2013, PP 139-147