Cued Click As An Authentication Mechanism For An Application

Ansari Sana Nafees Ahmed
Computer Engineering
Mohammed Haji Saboo Siddik College of Engineering
Mumbai, India

Shaikh Mohammed Sadique
Computer Engineering
Mohammed Haji Saboo Siddik College of Engineering
Mumbai, India

Shaikh Saubiya Ahmed
Computer Engineering
Mohammed Haji Saboo Siddik College of Engineering
Mumbai, India

Er. Shaikh Asadullah
Computer Engineering
Mohammed Haji Saboo Siddik College of Engineering
Mumbai, India

***Abstract* - Cued Click point is a click-based graphical image password technique which is a successor of pass point technique. Users now a day we have problems with recalling alpha-numerical passwords. To provide an alternative approach we propose using image based passwords. It is a human psychology that we tend to remember graphics or images rather than alpha-numerical text .Our main is to facilitate an easy way of authentication of the authorized person for any N number of applications. Initially the user has to register them self into the system and choose user defined or system defined images, that would be convenient to the user to recall them later on while logging in. The user selects cued points on an image which is divided into grids. The user then selects a point on an image as per his recalling abilities. To make the process difficult for an unauthorized user to log in , we allow the user to select the difficulty levels of the cued click password , by differing the size of the grids. If an unauthorized user attempts to log in to the system and exceeds more than the number of attempts granted by the system administrator then the system will enforce a shut down at the backend and alert the administrator of an intruder.**

Keywords: authentication, image-passwords, password, usability, security.

I. INTRODUCTION

Various image based password algorithms have been proposed as alternatives to text based passwords.

Initially the era of authentication came into existence when the World Wide Web became prevalent source for file sharing, electronic mails, social networking, bulletin boards, forums etc. for all these purpose the user required to prove that they are the legitimate user accessing their own account using their credentials. This gave rise to the use of text based passwords, which were first generation of passwords. Text based passwords were easy to recall and were easy for anybody to guess, via social engineering. And also text based passwords were susceptible to dictionary attacks, in which all the words which are there in dictionary can be used in a brute force attack.

The second generation of passwords includes texts along with numbers so that the complications for hacking a password increases, but unfortunately this technique wore out. The third generation of passwords includes alpha-numerical along with special characters, but this proved to be arduous for the user to recall while logging in.

Psychological studies on human brains have showcased that they tend to recall images and graphics more easily then alphanumeric or text. Passwords should be easy to recall when needed, as well as should be random in nature. The main problems of passwords are that they should be altered frequently, and should be distinct for every account that the user possesses. They should not be noted down or it should be made impregnable by using various cryptographic and steganographic algorithms.

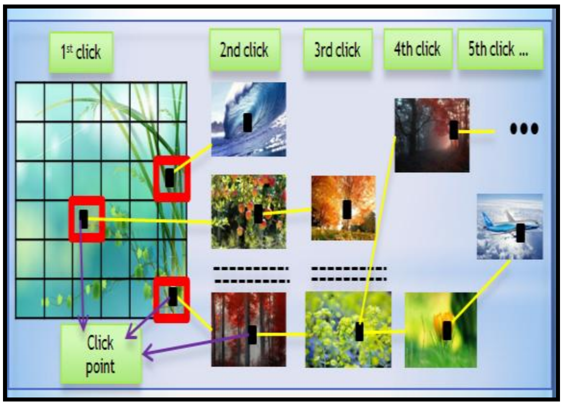


Fig 1:- Different Images with Click Points

In this project, we propose new way of authentication of authorized personnel via a click based graphical password application called Cued Click Points. It can be viewed as a combination of cued clicks on random images generated by the system at that instant. Users password consists of one click-point per image for a sequence of images selected by users it. 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 while login.

II. EXISTING SYSTEM

There are many ways of authenticating the legitimate user but each has its limitations and drawbacks, which can be used

By the attacker and they can exploit these limitations and make the system susceptible to intruders, or even leak of sensitive Information. Few methods are

- Token authentication
- Token with passkey
- Biometric authentication

Token is something which proves that the user has the rights to access to a certain facility, such as an identity card, RFID tags etc but the problem here is that a un authorized person can get his hands on these tokens and gain access to the facility or computing environment. This proved to be the major drawback of this token based authentication system.

To make this method more secure algorithms have been implemented to make this method secure via amalgamation of knowledge that only the legitimate user shall possess that can. So the tokens were used in combinations with keys and text based passwords.

The drawback of this technique was that an intruder can perform social engineering on his victim an can get access to the token (credit cards, smart cards etc) To overcome all these disadvantages biometric system was implemented, biometric uses the physical characteristics of the user stores them in the data base and who so ever wants to access the system is cross verified by the biometric tools such as fingerprint scanner, retina scanner etc which is unique for every one on this planet. the disadvantage was that these biometric equipments were expensive and the success ratio was also not good.

Most systems use passwords which are either token based or biometric based and they all have their drawbacks. An alternative approach was text based passwords but the problem with text based Passwords are with usability. The users tend to forget the passwords of their account.

III. DESIGN OF CUED CLICK POINTS

In Pass Point passwords technique a sequence of five click points on a given image. Users may select any spot on the image as click-points for their password. To log into the system, they enter the sequence of clicks in the correct order. Each click must be within a system-defined tolerance region or grid of the original click-point. The usability and security of this technique was evaluated by the original authors they found that although relatively usable, security problems still prevail. The primary security problem is critical regions: different users tend to select same click-points as part of their passwords on same image.

Attackers who acquire knowledge of this critical region through harvesting sample passwords or through by use of automated image processing techniques can build attack dictionaries and more successfully guess Pass Points password.

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, it is a kind of brute force attack but in a more systematic way.

Attacks can target a single account, or can try guessing passwords on a large number of accounts in hopes of getting access into any of them, leaving the whole system vulnerable to attacks from disparate sources. To reduce the security impact of critical regions and further improve usability, we proposed an alternative click-based graphical password scheme called Cued Click-Points.

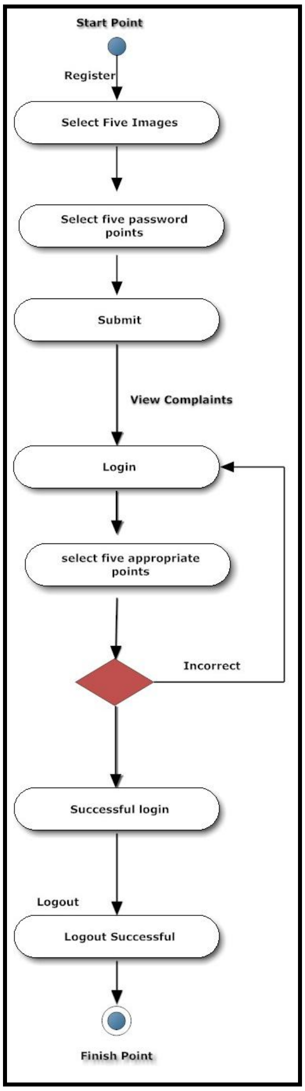


Fig 2:- Basic Design of Cued Click Points

IV. Proposed System

The proposed system aims at reducing the burden on user memory by recall and recognition based techniques. As the system we are trying to implement already exists. We've decided to tweak the system so as to make it unique in its implementation. The user must define the number of pictures that he can remember and must select either their sets of images of system images. Once they have selected "n" number of images that is feasible according to the recalled passwords.

The system will ask the user to enter AUTHENTIC points on the images, these points are nothing but they will authenticate the authorized user. The existing system only allow the user to enter the points with the help of the mouse regardless of that fact that the user can be shoulder surfed by the attacker or any unauthorized user. So as to protect the integrity of the system, we have introduced BOGUS-POINTS and password fields.

When the user is asked to enter the points for authentication he may enter n number of points on the image, in any Sequence. But the user should know the sequence of the correct point. Then the user must enter the correct sequence

In the password FEILD either in the form numbers ie.1, 2, 3, 4 or in the form of alphabets. FOUR, in this case four is the correct sequence. Even if the attacker is shoulder surfing the legitimate user he cannot gain access to the system because the user may enter n number of points and then, he may enter the sequence of the correct point in the password field. This will be repeated for N images that the user had selected.

V. Implementation

We were successful in creating a prototype of our proposed system. It has following modules.

1) Registration

2) Login

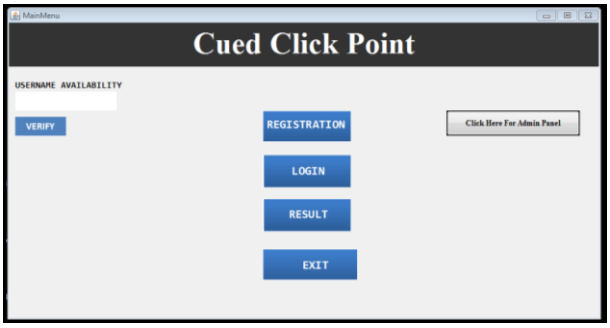


Fig 3:- Home Page Of Cued Click Points

a) Registration process

During the process of registration the user can select system defined pictures which are stored at the server side or the user has the freedom to select user defned images which are stored on the client machine. The user can select the mode of difficulty as per their convenience. the Difficulty levels aims at reducing the Hotspot of any cued click point on the image and render re usability useless.

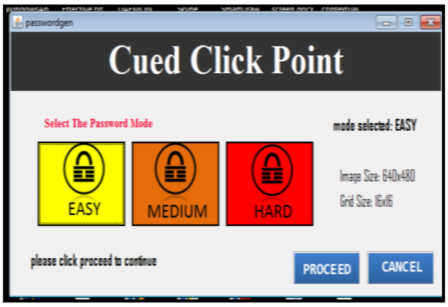
b) Mode Selection Process

There are 3 difficulty levels.

1) Easy

2) Normal

3) Hard



mode selected: EASY

Image Size: 640x480

Grid Size: 16x16

please click proceed to continue

Fig 4:- Mode Selection Tab Of Cued Click Points

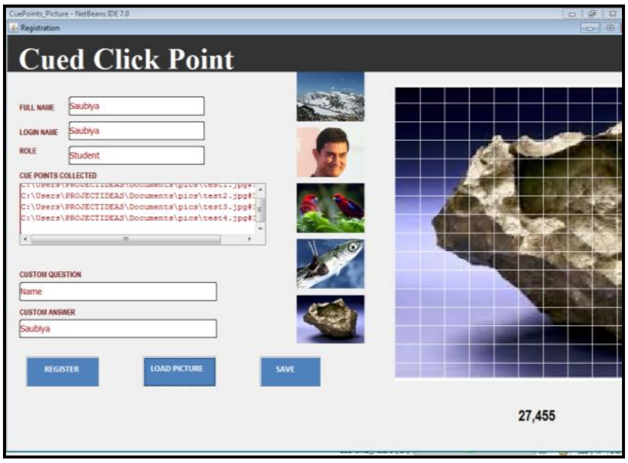
When the user selects easy difficulty and normal level based on that the image is segmented into 16*16 blocks also known as grid, the images which are used are of dimensions 680*480 pixels of resolution in jpg format. For normal level the image is divided into 30*30 grid and for hard level the image is divided into 40*40 grids thus depending upon the level of security needed the user can choose the difficulty level according to their convenience.

Why JPEG format?

JPEG uses a lossy form of compression based on the discrete cosine transform (DCT). This mathematical operation converts each frame/field of the video source from the spatial (2D) domain into the frequency domain (aka transform domain.) A perceptual model based loosely on the human psycho visual system discards high-frequency information, i.e. sharp transitions in intensity, and color hue. In the transform domain, the process of reducing information is called quantization. In simpler terms, quantization is a method for optimally reducing a large number scale (with different occurrences of each number) into a smaller one, and the transform-domain is a convenient representation of the image because the high-frequency coefficients, which contribute less to the over picture than other coefficients, are characteristically small-values with high compressibility. The quantized coefficients are then sequenced and losslessly packed into the output bit stream. Nearly all software implementations of JPEG permit user control over the compression-ratio (as well as other optional parameters), allowing the user to trade off picture-quality for smaller file size. In embedded applications (such as miniDV, which uses a similar DCT-compression scheme), the parameters are pre-selected and fixed for the application.

c) Selection Of Images

The user has to select 5 images and also click point on each image. These click points are then passed as on to the parameter for scrutinizing the user at the time of login. If the user at the time of login enters random click points on an image for more than 3 times the application will shut down and alert the server side for a possible intruder. In case the authorized user forgets the click point which he has saved, then he shall provide a answer to a secret questions which he had entered at the time of registration.



CuePoints_Picture - NetBeans IDE 7.0

Registration

Cued Click Point

FULL NAME: Saubiya

LOGIN NAME: Saubiya

ROLE: Student

CUE POINTS COLLECTED

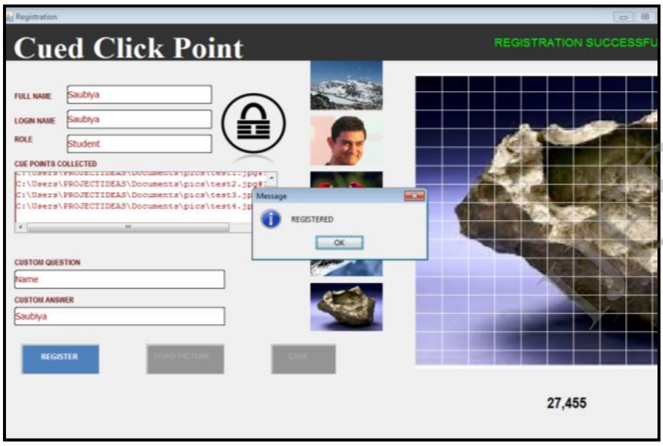
```
C:\Users\PROJECTIDEAS\Documents\pics\test2.jpg#
C:\Users\PROJECTIDEAS\Documents\pics\test3.jpg#
C:\Users\PROJECTIDEAS\Documents\pics\test4.jpg#
```

CUSTOM QUESTION: Name

CUSTOM ANSWER: Saubiya

27,455

Fig 5:- Selection Of Images while Registeration Cued Click Points



Registration

Cued Click Point

REGISTRATION SUCCESSFU

FULL NAME: Saubiya

LOGIN NAME: Saubiya

ROLE: Student

CUE POINTS COLLECTED

```
C:\Users\PROJECTIDEAS\Documents\pics\test2.jpg#
C:\Users\PROJECTIDEAS\Documents\pics\test3.jp
C:\Users\PROJECTIDEAS\Documents\pics\test4.jp
```

Message

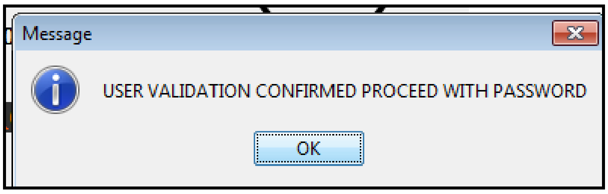
REGISTERED

CUSTOM QUESTION: Name

CUSTOM ANSWER: Saubiya

27,455

Fig 6:- Registeration Confirmed Of Cued Click Points



Message

USER VALIDATION CONFIRMED PROCEED WITH PASSWORD

Fig 7:- Checking Of Username Availability Cued Click Points

VI. Advantages & Disadvantages

- Graphical passwords may offer better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words (rather than the recommended jumble of characters).
- A dictionary search can often hit on a password and allow a hacker to gain entry into a system in seconds.
- But if a series of selectable 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.
- If there are 100 images on each of the 8 pages in an 8-image password, there are 100^8, or 10 quadrillion (10,000,000,000,000,000), possible combinations that could form the graphical password.
- If the system has a built-in delay of only 0.1 second following the selection of each image until the presentation of the next page, it would take (on average) millions of years to break into the system by hitting it with random image sequences.
- It is more difficult to carry out a brute force attack against graphical passwords than text-based passwords.
- A graphical password is easier than a text-based password for most people to remember.
- Suppose an 8-character password is necessary to gain entry into a particular computer network. Instead of w8KiJ72c, for example, a user might select images of the earth (from among a screen full of real and fictitious planets), the country of France (from a map of the world), the city of Nice (from a map of France), a white stucco house with arched doorways and red tiles on the roof, a green plastic cooler with a white lid, a package of Gouda cheese, a bottle of grape juice, and a pink paper cup with little green stars around its upper edge and three red bands around the middle.
- During the authentication, the user must enter the registered images in the correct sequence. One drawback of this technique is that since the number of thumb nail images is limited, the password space is small.
- Each thumbnail image is assigned a numerical value, and the sequence of selection will generate a numerical password.
- Text-based passwords have a password space of 94^N, where N is the length of the password, 94 is the number of Printable characters excluding SPACE.

VII. Conclusion And Future Work

The core element of computational trust is identity. Currently many authentication methods and techniques are available but each with its own advantages and shortcomings. There is a growing interest in using pictures as passwords rather than text passwords but very little research has been done on graphical based passwords so far.

In view of the above, we have proposed authentication system which is based on graphical password schemes. Although our system aims to reduce the problems with existing graphical based password schemes but it has also some limitations and issues like all the other graphical based password be more secure, reliable and robust as there is always a place for improvement.

Currently we are working on the System Implementation and Evaluation. In future some other important things regarding the performance of our system will be investigated like User Adoptability and Usability and Security of our system.

VIII. ACKNOWLEDGEMENT

We are thankful to Mohammed Haji Saboo Siddik College of Engineering, for providing us the opportunity to do constructive work. We also thank anonymous reviewers for their constructive suggestions.

IX. REFERENCES

1. Chiasson, S., Biddle, R., and van Oorschot, P.C. A Second Look at the Usability of Click-Based Graphical Passwords. 2007.
2. Cranor, L.F. and Garfinkel, S. (eds). *Security and Usability: Designing Secure Systems that People Can Use.* O'Reilley Media Inc, Sebastopol, CA, 2005.
3. Davis, D., Monrose, F., Reiter, M.K. On User Choice in Graphical Password Schemes. USENIX Security Symp. 2004.
4. Dirik, A.E., Memon, N., and Birget, J.C. Modeling user choice in the PassPoints graphical password scheme.2007.
5. Keith, M., Shao, B., and Steinbart, P.J. The usability of Passphrases for authentication: An empirical field study, Int. Journal of Human-Computer Studies, 65(1), 17- 28, 2007.
6. Kuo, C., Romanosky, S., and Cranor, L. F., Human Selection of Mnemonic Phrase-based Passwords, Symp. on Usable Privacy and Security (SOUPS), 2006.