IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

PASSWORD AUTHENTICATION BASED ON CUEPOINTS OF IMAGES

MYLABATHULA RATNA VIVEKA [#1], A. DURGA DEVI [#2]

[#1] MSC Student, Master of Computer Science,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Assistant Professor, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

ABSTRACT

Click Cued points are a click-based graphical password scheme, a cued-recall graphical password technique. User click on one point per image for a sequence of images. The next image is based on the previous click point. Users preferred CCP to pass point, Saying that selecting and remembering only one point per image was easier, and that seeing each image triggered in their memory of where the corresponding point was located. CCP also provides greater security than pass Points because the number of images increases the workload for attackers.

1. INTRODUCTION

Human factors are often considered the weakest link in a computer security system. Patrick, pointed out that there are three major areas where human computer interaction is important: authentication, security operations, and developing secure systems. Here we focus on the authentication problem. The most common computer authentication method for a user is to submit a user name and a text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also be easily guessed or broken. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for

different accounts. To address the problems with traditional username password authentication, the authentication methods were classified into following types:

1. Biometric,
2. Token based and
3. Knowledge Based authentications.

Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security.

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. This project is based on a new click-based graphical password scheme called Cued Click Points (CCP). It can be viewed as a combination of Pass Points, Pass faces, and Story.

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. Users could quickly create their password. Another feature of cued

2 click point is the immediate implicit feedback (Knowledge based feedback) telling the correct user whether their latest click-point was correctly entered.

Cued Click Points (CCP) is a proposed alternative to Pass Points. In CCP, users click one point on each of images rather than on different points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point at which point they can cancel their attempt and retry from the beginning. It also makes attacks based on hotspot analysis more challenging.

As shown in Figure 1, each click results in showing a next-image, in effect leading users down a “path” as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. If the user dislike the resulting images, they could create a new password involving different

images with different click points.

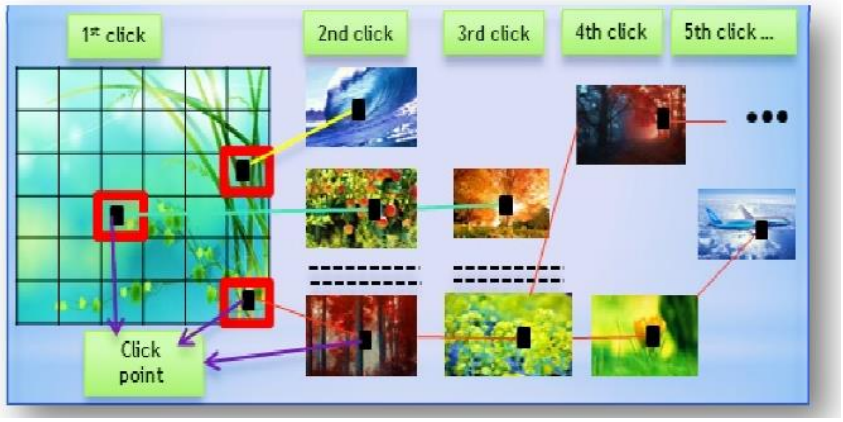


Fig. 1. CCP passwords can be regarded as a choice-dependent path of images.

During password creation, the first image can be selected by the user from the system (hard disk drive) .We will find out the co-ordinates of the click-point and will find out the tolerance square number. For each click-point in a subsequent login attempt, this number is retrieved and used to determine whether the click-point falls within tolerance of the original point.

3. This system is divided into 3 password sensibility (levels) namely easy, medium and hard. The images are of size 640x480 pixels and cells of 16x16,20x20, and 40x40 pixels. We have different layers of images each containing 256, 400, and 1600 squares. Let us consider easy mode where the image size is of 640x480 and 256 squares. We use a random function to maps each cell to a next-image. Each of the 256 next-images would have 256squares and thus require 256 next-images of their own. The number of images would quickly become quite large increasing exponentially. When computing the next-image index, if any is a repeat, we can select a distinct image using load picture button.

For example, if attackers identify five likely click-points on the first image, then they need to analyze the five corresponding second images (once they determine both the indices of these images and get access to the images themselves), and so on, growing exponentially. A major usability improvement over Pass Points is the fact that legitimate users get immediate feedback about an error when trying to log in. When they see an incorrect image, they know that the latest click-point was incorrect and can immediately cancel this attempt and try again from the beginning. The visual cue does not explicitly reveal “right” or “wrong” but is evident using knowledge only the legitimate user should possess. As with text passwords, Pass Points can only safely provide feedback at the end and cannot reveal the cause of error.

Algorithm for Creating grid on the panel

1. Consider variables x1 and y1.

2. Consider a variable named choice no (this variable will take grid size eg.16x16)

3. y1 will take the value for height such that height is divided with choice no similarly

x1 will take value for width such that width is divided with choice no.

4. Finally the lines are created by using drawline method.(the panel will contain total of 256 squares)

Algorithm for Accepting point on the grid

1. Take the variables dx and dy. The dx will take the panel x coordinate which will be subtracted f with the frame x coordinate.
2. dy will take the y co-ordinate value.
3. The point clicked will be taken by p.x where x is x coordinate of panel and p is point.

The p.x is subtracted with dx value this obtained value is placed into the variable x.similary we take value for y.

4. The obtained x value is now compared with the panel width which is obtained from getwidth ()/choiceno. If the value of x is less than the compared value then a variable code will collect the block values. Similarly y value is compared and the value store into code variable.
5. The block value is compared with the block value from the database.

PROBLEM STATEMENT

A user's initial image is selected by the system, based on user characteristic such as username. The sequence is regenerated on-the-fly from the function each time a user enters the password. If a user enters an incorrect click-point, then the sequence of images from that point onwards will be incorrect and thus the login attempt will fail. For an attacker who does not know the correct sequence of images, this cue will not be helpful. We expect that hotspots will appear as in Pass Points, but since the number of images is significantly increased, analysis will require more effort which increases proportionally with the configurable number of images in the system.

PURPOSE

Cued Click Points (CCP) is a proposed alternative to Pass Points. In CCP, users click one point on each of images rather than on different points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point at which point they can cancel their attempt and retry from the beginning. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. If the user dislike the resulting images, they could create a new password involving different images with different click points.

2. LITERATURE SURVEY

2.1 INRODUCTION

Literature survey is the most important step in software development process. Before developing the tool, it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, ten next steps are to determine which operating system and language used for developing the tool. Once the programmers start building the tool, the programmers need lot of external support. This support obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into for developing the proposed system.

2.2 RELATED WORK

DaeHun Nyang, proposed and analyzed the use of user driven visualization to improve security and user-friendliness of authentication protocols. They have shown two realizations of protocols that not only improve the user experience but also resist challenging attacks, such as the keylogger and malware attacks. Proposed protocols utilize simple technologies available in most out-of-the-box smart phone devices. Author developed Android application of a prototype of our protocol and demonstrate its feasibility and potential in real-world [5].

M. Mannan, has implemented a simple approach of Mobile Password Authentication. While PC's tend to dominate transaction processes they are vulnerable to various forms of attacks so they have used an intermediate device in the form of mobile and hence security is not entirely dependent on PC's [6].

Haichang Gao, have put forth the idea of including graphical password strategy for authentication. Their paper presents the idea that long alphanumeric passwords are hard for people to remember while shorter is easy to crack so a conclusion is to include graphical password [7].

R Divya, proposed system consisting of two protocols for authentication which resisted keylogging. The two authentication protocols are Time based One-Time- Password protocol and Password-based authentication protocol. Their proposed system shows how visualization can enhance usability and security[8].

3. EXISTING SYSTEM

In existing system user can provides security through either

1. Textual Password (Or)
2. Using Graphical Image System.

existing system uses Pass Points (which was created to overcome text password authentication problems) concept. It proposed Passwords which could be composed of several points anywhere on an image. Passwords consist of a sequence of five click points on a given image. Users may select any pixel in the image as click-point for their password. To log in, they repeat the sequence of clicks in the correct order. Each click

must be within a system-defined region of the original click-point. There was no which can take cue click point as authentication.

LIMITATION OF EXISTING SYSTEM

1) The following are the various limitations or drawbacks of the existing system
2) Data Lose
3) Hacking of System Data.
4) Easy to Break the Text Based Passwords with a Very Lees Effort.
5) There was also a severe problem for remembering Random passwords which was generated by the System.

4. PROPOSED SYSTEM

CCP uses one click-point on each of a sequence of five images. The next image displayed is determined by the location of the previously entered click-point. The claimed advantages are that logging on becomes a true cued-recall scenario, wherein seeing each image triggers the memory of a corresponding click-point. Thus remembering the order of the click-points is no longer a requirement on users, as the system presents the images one at a time. When logging on, if users suddenly see an image they do not recognize, they know that their previous click-point was incorrect. However, to an attacker without knowledge of the correct password, this cue is meaningless.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system, they are as follows:

1. Graphical password schemes provide a way of making more human-friendly passwords.
2. Easy to remember and hard crack.
3. It made use of immediate implicit feedback or knowledge based feedback method.
4. Fast login time than the pass point system.
5. Highly secured than the text password.

The username allows for retrieval of only the first image, which provides only limited information to an attacker

5. SOFTWARE PROJECT MODULES

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. The proposed application is divided into mainly 2 modules and they are many sub-modules present in these main modules. Now let us look about them in detail as follows:

1) User Registration Module
2) User Login Module

5.1 USER REGISTRATION MODULE

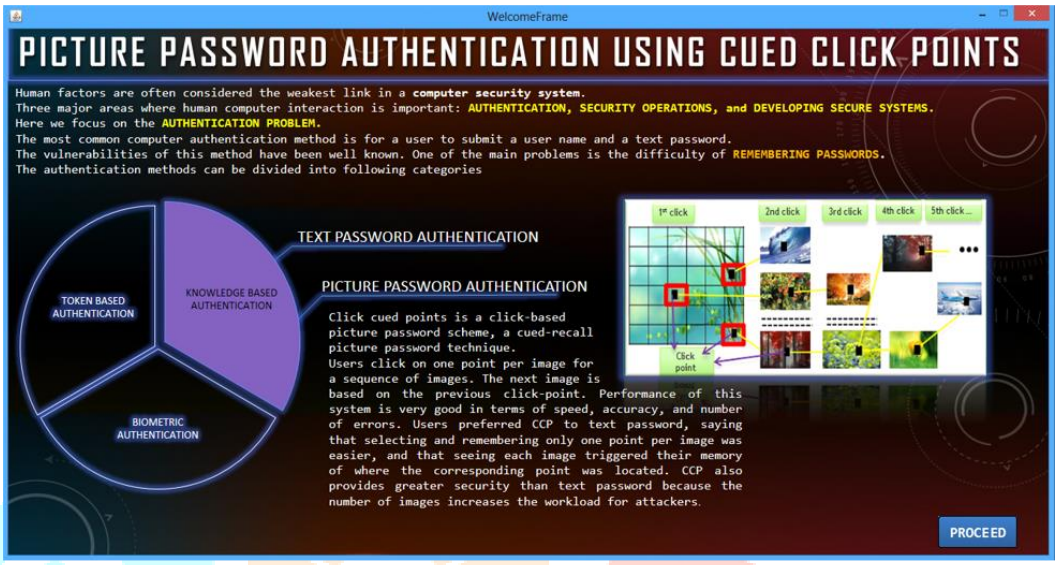
1. User fills the registration form.
2. User click on the Load Picture button for selecting picture.
3. User click one point on the picture and click on Save button.
4. The user repeats above process until he reaches last picture.
5. Once the user completes all pictures and their associated click points, then he click on Register Button.

5.2 USER LOGIN MODULE

1. User enters the user name.
2. User click on Verify Button for verification.
3. User selects the feedback method.
4. User click on Proceed Button to enter into user password picture.
5. User click on the picture.

6. RESULTS

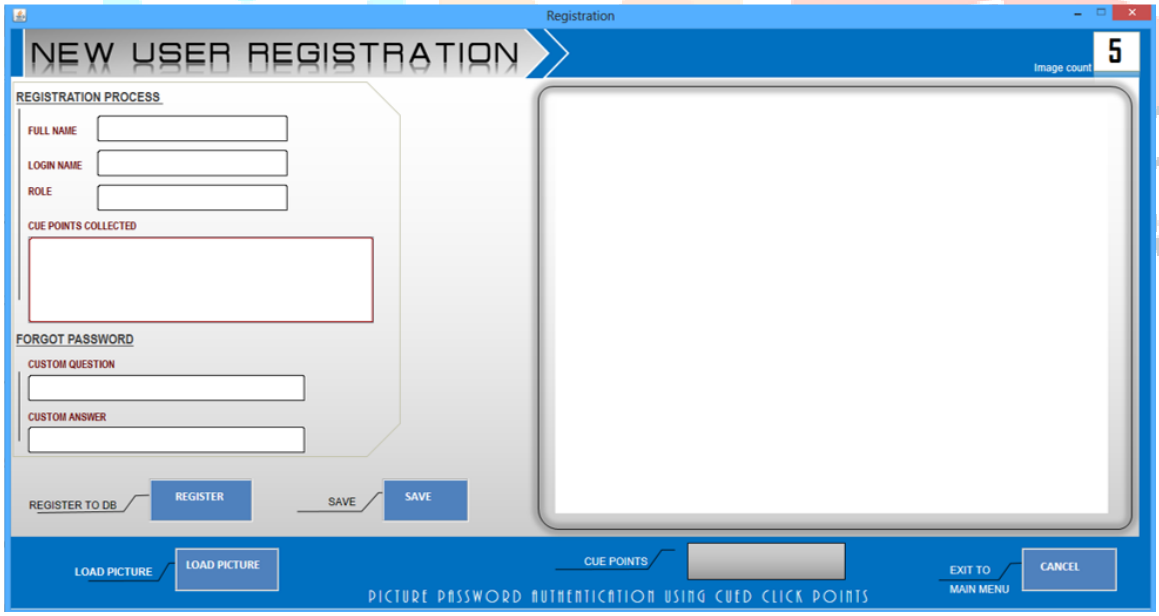
WELCOME FORM:



MAIN MENU:

PASSWORD LEVEL:

REGISTRATION FORM:



REGISTRATION FORM: PICTURE PASSWORD

User password pictures are over for cue points

SUCCESSFUL REGISTRATION GIVE ACCESS TO USER ACCOUNT

User successfully registered. The system opens user account.

7.CONCLUSION

The project provides an easy way to remember passwords by clicking on the desired cuepoints,which are easy to track as compared to handle text based passwords.The cuepoints are used as an modification version of passpoints used in current operating system.Cuepoints enables all ages of people to remember the password by cuepoints which are squared blocks created according to the mode of password generation selected by the user.

8. REFERENCES

[1] “Persuasive Cued Click-Points:Design, implementation, and evaluation of a knowledge-based authentication mechanism” Sonia Chiasson, Member, IEEE,Elizabeth Stobert, Alain Forget, Robert Biddle, Member, IEEE, and P. C. vanOorschot, Member, IEEE,2010

[2] Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," *Communications of the ACM*, vol. 42, pp. 41-46, 1999.

[3] S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot. “Influencing userstowards better passwords: Persuasive Cued Click-Points. In Human Computer Interaction(HCI),” The British Computer Society, September 2008.

[4] Dhamija, R. and Perrig, A. (2000). Déjà Vu: “User study using images for authentication. In *Ninth Usenix Security Symposium*.”

[5] S. Akula and V. Devisetty, "Image Based Registration and Authentication System,"in *Proceedings of Midwest Instruction and Computing Symposium*, 2004.

[6] M. Kotadia, "Microsoft: Write down your passwords," in *ZDNet Australia, May 23*,2005.

[7] S. Chakrabarti and M. Singhal. “Password-based authentication: Preventing dictionary attacks.” Computer, IEEE Computer Society, 40(6):68{74, June 2007.