OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

PREVENTION AGAINST ONLINE PASSWORD GUESSING ATTACKS USING IMAGE BASED AUTHENTICATION TECHNIQUE PCCP

Ms. Jyoti Madhukar Shinde

Department of Computer science engineering, Ambarwadikar Institute of Technology, Aurangabad, Maharashtra, India.
shinde.jyoti1486@gmail.com

Abstract: Knowledge based authentication systems support user for selecting password for higher security. To show effected user choice, encouraging users for selecting random points click based graphical passwords is used using click points. To protect the Passwords theft it is useful. Now Before allowing users to access the services Text based username password used in authenticating users. To overcome from this problem is to assign random password to the user. But it is difficult for human in recalling a random password string. So user will then write it down. Another drawback with text is it is crack by telling to friend. This paper based on knowledge based authentication. Authentication protects the resources from unauthorized user. Text based passwords are not secured for many application so Image based Authentication (IBA) is used which is based on user's identification of image based click points password. After user name enter in to the authentication module, it respond by displaying an image which contains click based approach in image match with other images from the user's password set

Keywords: *PPS (Pass-point Scheme), CCP (Cued click points), PCCP (Persuasive Cued Click Points), CTS Common Type System, IBRAS (Image Based Registration and Authentication System)*

I INTRODUCTION

From last few decades authentication method is get used that make use of text based password. For ease of remember and due to conscious knowledge about how tracker tend to attack user go with short password. To overcome with this problem latest technique have been proposed using Graphical as passwords. The founder of graphical password was described by Greg Blonder (1996). Psychologically humans can easily remember graphical far better than text and hence it is the best alternative being proposed for online security purpose. The main aim of this project is to minimize the guessing attacks and motivate the user can select more random and un guessing password to guess.

Objective:

The main aim of the Image based authentication technique is to guide the users in generating password for higher security. Here we use persuasion in click based graphical passwords, motivating users for selecting random & complicated to guess click points. This project report paper proposed the method for authenticating users not by text but through graphical image selection.

II LITERATURE SURVEY

Authentication:

In Authentication user present some credential to the system if the user credential recognizes by system or match with system provided data then only user considered as authorized user otherwise not. Every new user must need to be get registered on system By providing user id and any other information to prove that user is authorized person before requesting services.

Types of Authentication:

1 Password Based Authentication System:

The password based user authentication system uses username and a password as a requirement for creating login. If username and entered password similar with the same data stored on the system database then only user get login and called authorized user. As users have more than one account

on many computers he has to remember many passwords also. But as per human remembering ability it is difficult to remember all passwords to human brain as per research on human cognitive ability [1].

2. Biometric Based Authentication System:

Biometrics, identify individual user by their biological or physiological characteristics which is new aspect in security system now a day. Using traditional security method user need to keep in mind password safe [3] using biometric it is not required. Biometric is quite safe and secure, reliable but costly need hardware and software support. This system are hard to maintain and change Deploying such system for internet application may be very complex

Image Based Password Techniques:

Different Graphical Password techniques are

1. Pass-point Scheme,
2. Cued-click point Scheme,
3. Persuasive Cued-Click Point Scheme.

1 Pass-point Scheme:

S. Wiedenbeck et al. proposed Pass-point scheme. In which a series of 5 different click points are consisted by a given image. For creating a password user select any sequence of 5 pixels in the image as a cloud lick point on same image and for login the user has to enter the same series of clicks in a correct sequence on the image. then get further access to the system.

The main drawback with this scheme is the HOTSPOTS because it is very easy for attackers to predict the pixel points selected as password as user forms specific patterns to remember the secret code which result the pattern formation make easy for attackers to guess.

2 Cued-Click Points:

Cued Click Point scheme was designed to minimize patterns and the use of hotspots for attackers. Inspire of selected 5 click-points on one image, CCP technique uses one click-point on 5 different images. The next image in series is based on the location of the former entered click-point; it creates a sequence through an image series. One of the best features of Cued-Click Point is that it shows authentication failure only after clicking final click-point, to protect from guessing attacks. Disadvantages Of these techniques are like false accept and false reject.

3 Persuasive Cued Click Points:

Persuasive Cued click points is technique in which persuasive feature is included into cued click point for selecting less predictable password. PCCP uses viewport and shuffle for password creation.

While creating password images are lightly highlighted exclude for viewport which are randomly positioned to avoid known hotspots. The benefit of PCCP is password theft have to improve their guesses where users have to choice a click points within the selected viewports and after clicking on shuffle button click outside of the viewport for randomly positioned the view port. PCCP technique is suffered from security problem at some level.

III SYSTEM ANALYSIS

For Existing System:

Existing system approaches to users to generate password which are very easy to find out for attackers and system generated password are difficult to remember for user. As per user natural tendency user always prefers short password for ease of remember and due to lack of knowledge about how attackers attacks on system. These passwords are guess by attackers using simple means like masquerading, Eaves drop and other means like dictionary attacks, shoulder surfing attacks.

For Proposed System:

We propose the image based password mechanism to reduce the guessing attacks and help encouraging users for selecting more random, and hard passwords to guess. As Human brain good in memorizing images than textual characters so it is easy to remember password to them.

IV SYSTEM ARCHITECTURE

Every system has graphical user interface which is very user friendly ease of use. The main page has the options for a existing user and a new user. Every new user has to register before he can log in to the system. He is registered using his Personal information like first, middle, last name, user name an image etc. all the fields are required filed except middle name. Once the user selected an image it is get displayed on the screen to verify his image. Image selection is users choice get his own image from external storage devices..SHA-1 algorithm produces output which is very secure and need less memory. This system is implemented using java platform. Figure 1 shows class interaction diagram for IBRAS.

Figure 2 shows Use Case Diagram Which shows the user and admin access to the system user registered using image and username create password .uses different authentication method for it and get login. Admin verify the username password and image click points with user created username and click points. And upload the profile and file. After that logout successfully.

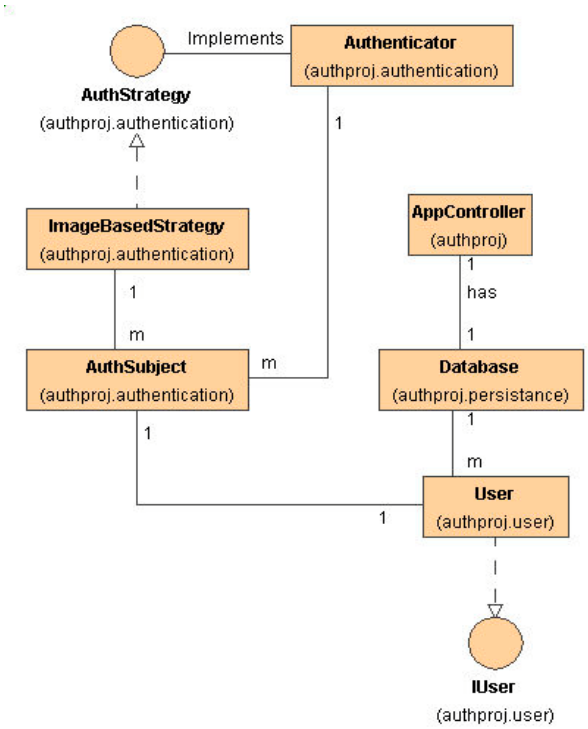
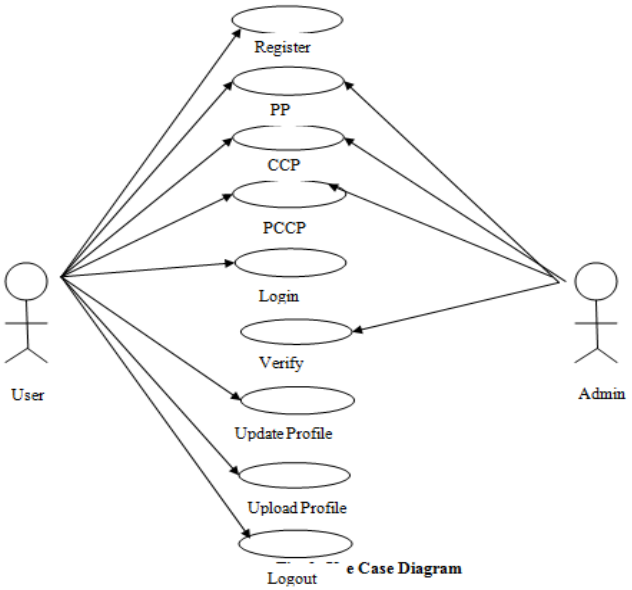


Figure 1 Class diagram on the IBRAS



e Case Diagram

Below are snapshots of the forms to explain PCCP authentication method in Which new user first register them self first then create password based on image by clicking on different images then he get the access to the home page if he is authorized user otherwise not.

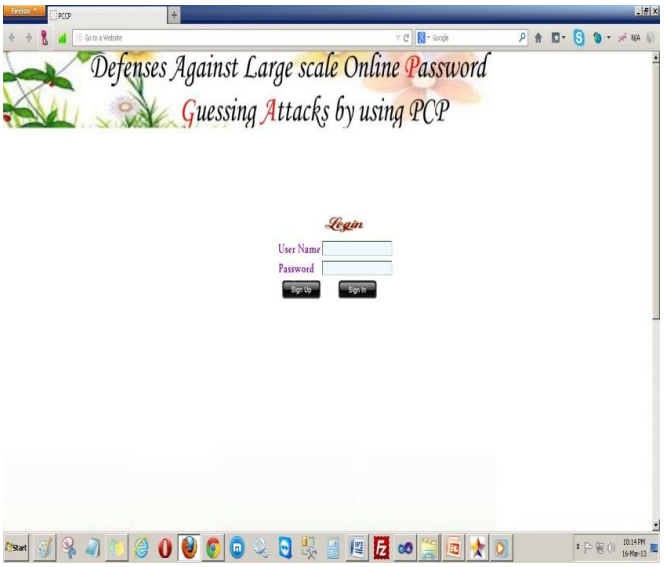


Figure 3 Login Page

On this Page Existing user can login successfully by entering their user name and password after clicking sign in button he/she goes to next page i.e. Image authentication page shown by Figure 5 for clicking on image viewpoint.If user is new user then he would register himself by entering his/her basic information on Registration form shown in Figure 4and after that click on images for selecting click points in series shown on figure 5

Figure 4 Registration Form

Registration form is for new user to register them self on system.

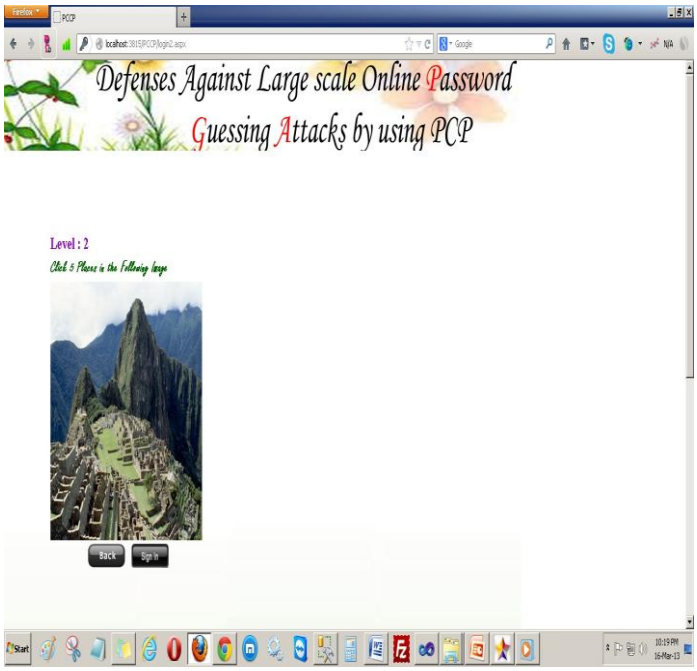


Figure 5 Cued Click point on image

After clicking On 5 different images Click points password get set for new user and for existing user password get verified by system to find is user authenticated or not?

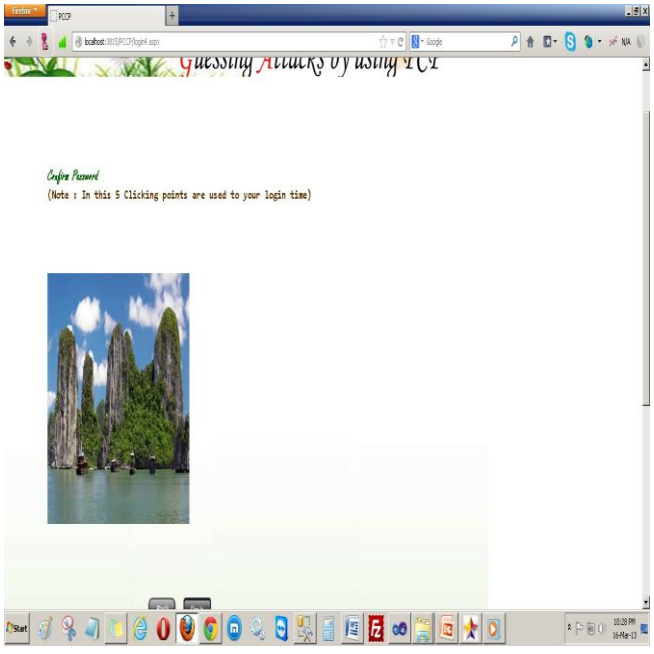


Figure 6 Confirm Password

After clicking on images click points if user is authenticated and password is get confirmed then system provide services to the authenticated user. Otherwise display message user in not authenticated.

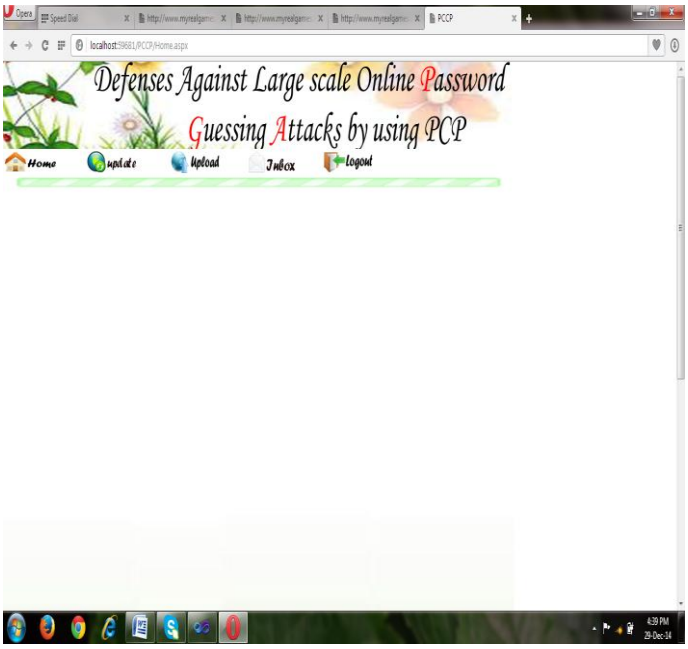


Figure 7 Home Page

After Login successfully user goes on Home Page for further service access.

V CONCLUSION

Graphical image based passwords are better to remember than Text based passwords, people are able to keep easily in mind graphical passwords than text-based passwords.

In contrast to brute force and dictionary attacks PGRP is more astringent by allowing a large number of free failed attempts for users. PCCP is most effective in avoiding password guessing attacks and provide convenient login PGRP suitable for both large and small number of user accounts.

Future Scope:

In future this system is to rebuilt by using object oriented methodology using required popular design pattern. JDBC connectivity is used to connect the relational database with the system. In future this work would be focused on betterment of the database by providing lifelong storage. The proposed system is developed as a standalone application which wills be deployed on internet easily, Also integrated with biometric systems to improve the security feature of the system. The system most useful for small scale devices like PDA's cell phones.

ACKNOWLEDGEMENT

It has been an overwhelming experience to develop this project report. It has helped me to gather information about various aspects of the working of the institute and has

broadened my vision on the applicability and implementation of this system. No words are good enough to express my gratitude and sincere thanks to our respected Principal Dr. Shelake Sir for his kind blessing, inspiration and providing the necessary support. I feel great pleasure in expressing my gratitude and sincere thanks to our Head of Department Prof Auti Sir for the approval of this project and his much needed guidance and encouragement. I thankful to my respected Project guide Prof. Saad Sdhiqui without whose kindness & valuable guidance the success of this project would have remained a dream.

I grateful to all staff members of Computer Science & Engineering department for their timely help. Last but not the least; I would like to thank all teaching and nonteaching staff members of my department who helped me for completing task successfully directly or indirectly.

REFERENCES

[1] A. Josang and G. Sanderud, "Security in Mobile Communications: Challenges and Opportunities," in Proc. of the Australasian Information Security workshop conference on ACSW frontiers, 43-48, 2003.

[2] B. Schneier, "Image Authentication: Too Little, Too Late," in Inside Risks 178, Comm's of ACM, 48(4), April 2005.

[3] D. Ilett, "US Bank Gives Image Authentication to Millions of Customers," 2005.

[4]. D.de Borde," Graphical Authentication," Siemens Enterprise Communications UK Security Solutions, 2008.

[5]. A. Herzberg, "Payments and Banking with Mobile Personal Devices," Comm's of ACM, 46(5), 53-58, May 2003.

[6]. J. Brainard, A. Juels, R. L. Rivest, M. Szydlo and M. Yung, "Fourth- Factor Authentication: Somebody You Know," ACM CCS, 168-78.2006.

[7]. N. Mallat, M. Rossi, and V. Tuunainen, "Mobile Banking Services," Communications of ACM, 47(8), 42-46, May 2004

[8]. "RSA Security Selected by National Bank of Abu Dhabi to Protect Online Banking Customers," 2005