THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Graphical Password Authentication: Implementation and Evaluation of Personalized Persuasive Cued Click Points

Asher D'Mello
BE, Department of Computer Engineering, St. Francis Institute of Technology, Mumbai, Maharashtra, India
Rohan Bagwe
BE, Department of Computer Engineering, St. Francis Institute of Technology, Mumbai, Maharashtra, India
Victor Fernandes
BE, Department of Computer Engineering, St. Francis Institute of Technology, Mumbai, Maharashtra, India
Ankita Karia
Assistant Professor, Computer Engineering, St. Francis Institute of Technology, Mumbai, Maharashtra, India

Abstract:
Persuasive Cued Click-Points (PCCP) is an integrated evaluation of the graphical password scheme, including usability and security evaluations, and implementation considerations. The systematic examination provides a comprehensive and integrated evaluation of PCCP covering both usability and security issues. An important usability goal for knowledge-based authentication systems is to support users in selecting passwords of higher security, in the sense of being from an expanded effective security space. This research work explores the possibility of designing and constructing a module that is easily pluggable into the existing authentication systems being used as of now. The working prototype is an open source simulation consisting of all the necessary modules to build the authentication system. This system is built using Java and Oracle 10g Express Edition as the database although most database systems can be used.

Keywords: *authentication, computer security, graphical passwords, guessing attacks and centered discretization, cued click points, graphical passwords implementation*

1. Introduction

When it comes to digital security, passwords have played a major role in our lives. When it comes to passwords, we need to remember that a password acts as an interface between a human and a computer. Therefore passwords should be such that can be easily processed in binary form by computers as well as easily usable by humans. Based on these constraints the options available for passwords are limited. The biggest challenge while researching a user authentication technique is coming up with a solution that maximizes the constraints of both security and user-friendliness. The concept of using images as passwords thus proves to be a good option as images are easy to remember by humans as Psychology studies have also revealed that the human brain is better at recognizing and recalling images than text [3]. While it also provides a large password sample set that enhances security.
This research is going to be an extension to the previously published topic "Graphical Password Authentication: Personalized Cued Click Points to overcome the limitations of Persuasive Cued Click Points." In the September, 2014 edition of the The International Journal of Science & Technoledge.

1.1. Graphical Passwords

"Graphical passwords are an alternative to alphanumeric passwords in which users click on images to authenticate themselves rather than type alphanumeric strings."[2] Traditional alphanumeric passwords while being the conventional form of digital authentication have drawbacks from a usability point of view. [2] Thus we focus on using graphical passwords as a better alternative when it comes to authentication.

1.2. Types of Graphical Passwords

Based on its implementation, graphical passwords have several classifications. We are not going to focus on all of them at this point as its already established earlier that several systems have too many disadvantages to be deployed into a real life production environment. [7]

1.2.1. Passpoints

In the pass point authentication scheme, the user clicks on multiple pixels on the screen to set it as his password. There is a tolerance value around each pixel calculated. In order to authenticate, the user needs to click on the appropriate pixel within the image in the correct sequence [5]. We are not going to implement passpoints due to its drawbacks such as hotspots and shoulder surfing.

1.2.2. Cued Click Points

In Cued click points there are a number of images used. During the registration phase, the user clicks on a point on an image and he is taken to another image, he again repeats this step for a predetermined number of images.[5] During the authentication phase the user is required to select on the appropriate pixels and based on a suitable tolerance value. If the pixel is correct, the user is authenticated. One of the major drawbacks of this system is Hot Spots which is taken care of by using Personalized Cued Click Points. Cued Click points offer great security however does not solve the problem of hotspots or shoulder surfing [6]. For this reason we have decided to build our project using Persuasive cued click points (PCCP).

1.2.3. Persuasive Cued Click Points

In Persuasive Cued Click Points, the system presents a view port to the user in addition to the process in cued click points, this fairly reduces the problem of hot spots. This however also makes the password moderately difficult to remember as the viewport is no longer visible during the authentication phase.[7] In additional to using Persuasive Cued Click Points, we provide the user with an option to upload the image of his own choice. This adds a touch of personalization to the password and also makes it easier to remember by the user without affecting the difficulty faced by an attacker to guess the password.

1.3. Acknowledgement

We would like to express our special thanks of gratitude to our project guide Ms. Ankita R Karia (Lecturer, St Francis Institute of Technology) for her help and support while researching on the subject. We would also like to mention that this would not be possible without the unity and cooperation of the authors Victor Fernandes, Asher D'Mello and Rohan Bagwe.

2. Previous Research

As already described earlier in the published topic "Graphical Password Authentication: Personalized Cued Click Points to overcome the limitations of Persuasive Cued Click Points." In the September, 2014 edition of the The International Journal Of Science & Technoledge, there is a growing demand in the use of alternate forms of more secure authentication systems as compared to the conventional alpha numeric system. Despite its advantages over other existing authentication schemes, PCCP has not been able to find its way into the production environment yet. The primary reason for this is that most existing systems have been transformed into rigid modules over time that they lack the adaptability property. We aim at providing a module that easily plugs into any existing project in such a way that it performs independently as well as seamlessly blends into the base program.

3. System Analysis

The primary goal of our proposed system was to easily integerate into any existing authentication system or atleast provide a framework for developers to build upon. Based on these conditions, the system had to adhere to a certain set of requirements.

3.1. Functional Requirements

Depending on what functionality we have expected our module to possess, we have laid down strict functional requirements.

- Cross platform compatibility: Though our simulation engine runs on Java, the code and algorithms used in the system are cross platform compatible as long as the base language chosen by the developer supports database connectivity and OOP.
- Database Integration: The database chosen here is the Oracle 10g Express Edition however, depending upon the scaling constraints of the developer, any suitable database module may be chosen.
- APIs and other Interfaces: The application can be run over 3rd party APIs however the discussion of the use of API's has been limited due to the fact that using a 3rd party server for the purpose of security and authentication introduces a high deal of risk and network issues such as network latency delays.

3.2. Non Functional Requirements

In systems engineering and requirements engineering, a non-functional requirement is a requirement that specifies criteria that can be used to judge the operation of a system, rather than specific behaviors. This should be contrasted with functional requirements that define specific behavior or functions. [4] Based on the system, its non functional requirements are:

- Availability: System should be available 24 x 7 x 365. Downtimes may make authentication impossible and also turn the system unresponsive while partial failures can compromise security.
- Accessibility: System should be accessible from any System. Most systems today are accessible via both desktop applications as well as portable devices such as phones mainly via a web interface. This makes the authentication process easier for the user while also distributing the system load across multiple applications and devices.
- Capacity: System should be capable of authenticating maximum number of users at any point of time. Also the system should easily be able to store the uploaded images by the users.

- Efficiency: System should produce accurate result with less resources. In this case the algorithm used should be optimized well and minimum queries need to be made to the database.
- Maintainability: System should be easy to maintain. There should be no or minimal downtime in the event of maintenance.
- Responsive: Time lag for Authentication (Registration and Login) should be as less as possible.
- Performance: System should provide high performance each time. The word high here is relative to the base system. Basically the authentication system used should be fast enough that it can keep up with the base program.
- Reliability: System should give accurate output every time. When it comes to security and user authentication, we cannot afford to have any compromise on reliability.
- Scalability: System should be easily scalable for future enhancements such as increase features such as a change password option or edit user details.

3.3. Use Case and System Description

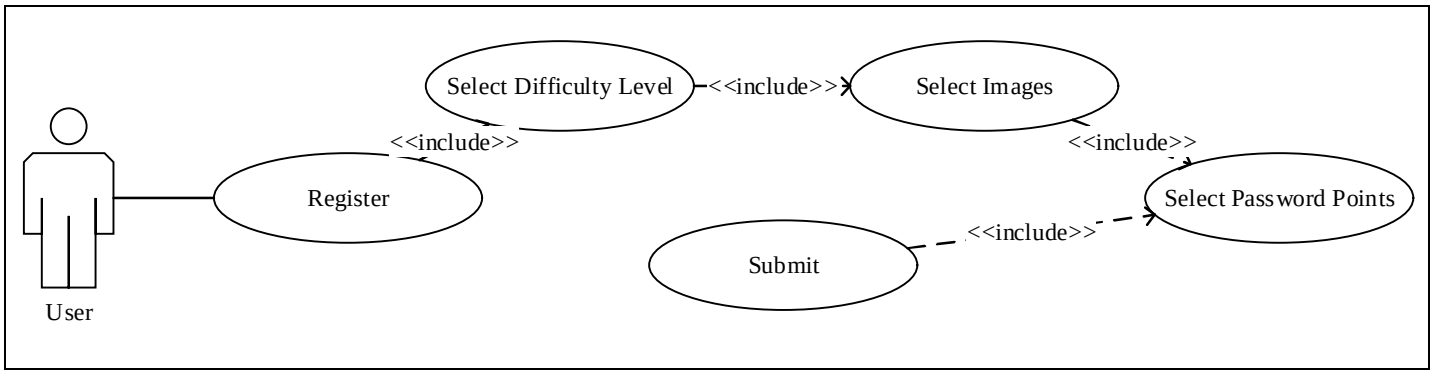

Figure 1: Use Case Diagram: Registration

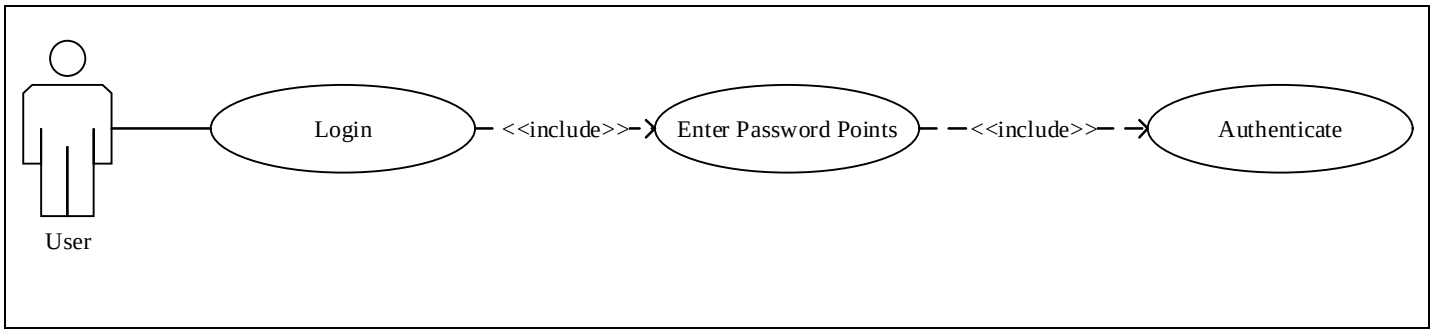

Figure 2: Use Case Diagram: Login

As shown above, the user can perform two activities, namely, register and login. The user can login only after registration. In registration phase, the user first selects the difficulty level, then the images from the system, and then selects points on the images and submits it. At the time of login, the user is given the images, and if user selects the correct points, he is authenticated.

3.4. System Architecture

Image based authentication system using persuasive cued click points consists of 3 phases as shown in Figure 3, It includes registration phase, security level selection phase, and login phase.

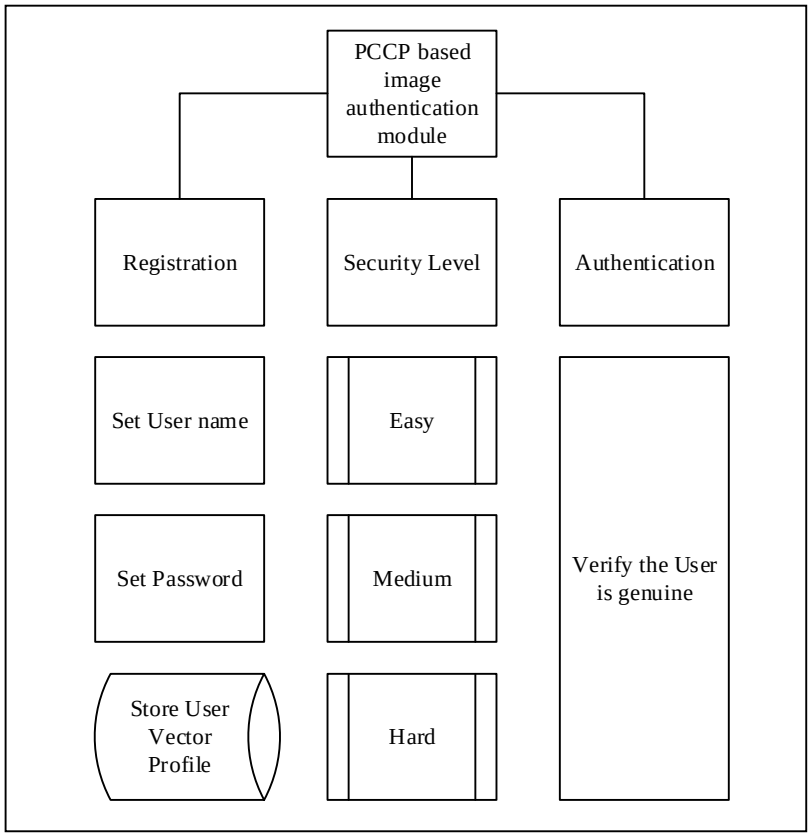

Figure 3: System Modules

3.4.1. Registration Module

In the registration phase, as shown in Figure 4, user selects a username which has to be unique. He selects the level of security as low, medium or high. He then selects the images accordingly, from the system and a password point on each image.

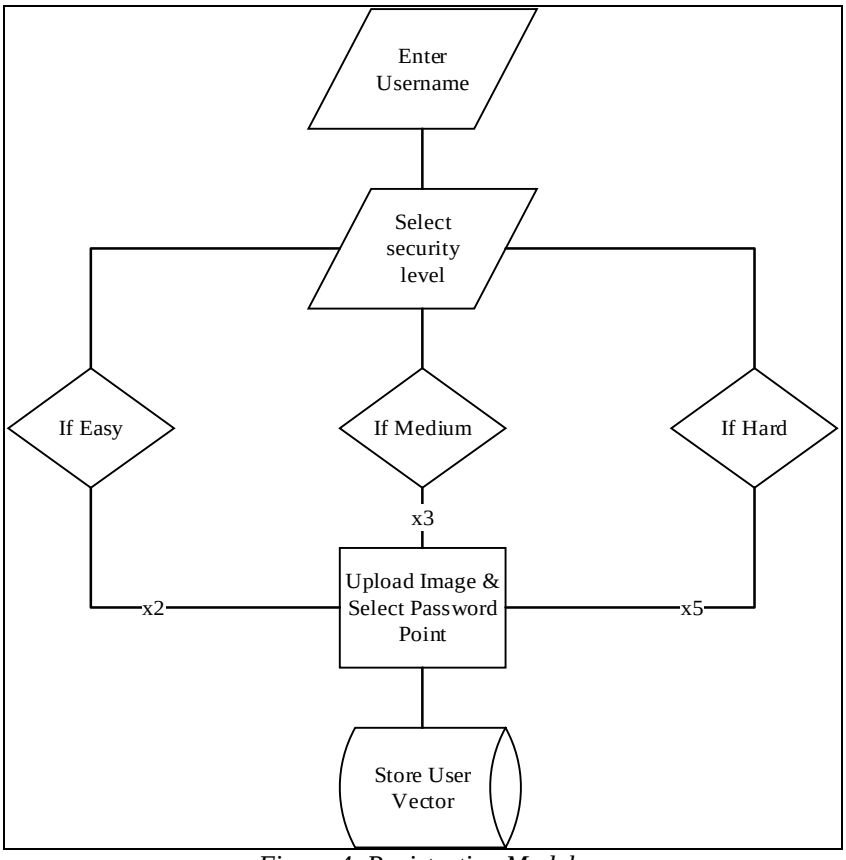

Figure 4: Registration Module

3.4.2. Login Module

In the login phase, as shown in Figure 5, user first enters his username. Then the user is presented with the first image which he had used during registration time. While logging, the viewport will not be visible and the user has to click on his registered click-point on the image. Since it is practically impossible for a person to click on the exact point, hence a tolerance value is hard coded in the system. The tolerance value (D) indicates the degree of closeness to the actual click-point. Euclidean distance is calculated to find the distance between two click points. Euclidean distance between two points' p and q is given by the following equation: $D (p , q) = [(p_1 – q_1) + (p_2 – q_2)]^{1/2}$

Above distance is calculated for each image and if this distance comes out less than a tolerance value D then only next registered image is displayed. The value of D is predefined in our system. Thus, if the click-point falls within the system defined tolerance area then only the next correct image will be displayed to the user, else a random image will be displayed.

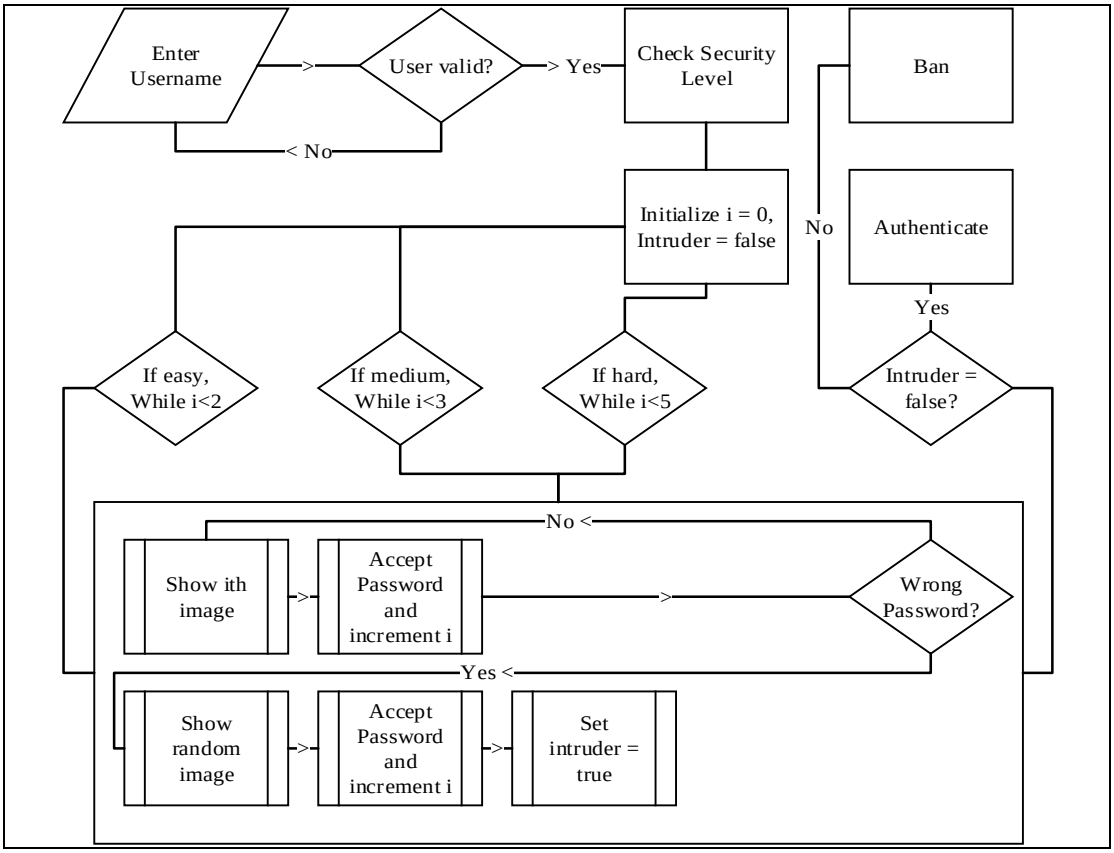

Figure 5: Login Module

4. Result

The system should function as an independent module having its own error management system built in at the same time also seamlessly integerate into the base application. For this purpose the proposed software has been through software testing so that the stakeholders and developers are assured about the quality of the software and the algorithms being implemented. Software testing also helps us understand an independent and purely objective view of the implementation. Test techniques include, but are not limited to, the process of executing a program or application with the intent of finding software bugs.

Test Case (Action performed)	Expected Result	Actual Outcome	Result
Existing username entered	Display message: user name exists	Message displayed	Pass
Unique user name entered	Display message: user name available	Message displayed	Pass
Incomplete details filled	Display message: missing data	Message displayed	Pass
User clicks on load image	Windows explorer opens	Windows explorer opens	Pass
User selects image	Image is loaded	Image is loaded	Pass
Viewport visible, user clicks shuffle	Viewport shuffles, infinite times	Viewport shuffles, infinite times	Pass
User selects password point inside viewport	Coordinates displayed	Coordinates displayed	Pass
User clicks outside viewport	Display message: select point inside viewport	Message displayed	Pass
User clicks save	Image link with coordinates saved and displayed	Image link with coordinates saved and displayed	Pass
Registration complete	Display welcome message	Message displayed	Pass

Table 1: Registration test cases

Test Case (Action performed)	Expected Result	Actual Outcome	Result
Login name entered	Verify from database and display message	Verified and message displayed	Pass
Click on proceed	First image must load from database	First image loads from database	Pass
Correct password point clicked	Display next correct image from database	Next image displayed	Pass
Incorrect password point clicked	Load a random image	Load a random image	Pass
Select a point on random incorrect image	Display next random image	Next random image displayed	Pass
Select a point on the last random incorrect image	Display message: Intruder detected	Message displayed	Pass
User selects all points correctly	Authenticate User , display welcome message	User authenticated, Message displayed	Pass

Table 2: Login test cases

5. Conclusion

The primary goal of this project was to increase the system security and also make it more user friendly. This has been achieved by using Persuasive cued click points in the form of a graphical password and also the effective password space has been increased. Furthermore, as previously stated giving the user a choice to upload his own set of images also adds to the security.

6. Project Contribution

Currently the project is live on GIT and will undergo a series of version iterations. Planned module specific updates are on the cards and will be updated in the same repository. The Source Files can be downloaded here: https://github.com/vicfdes/pccp

7. Future Work

The project is currently in a simulation stage which we intend making available to other platforms. We have planned developing a php module that integerates into codeigniter so that developers can easily install the graphical authentication system into their projects. We also plan on increasing the scalability of the prototype by giving developers an option to change the password difficulty levels as well as vary the number of images and viewports. Currently our application supports an unlimited chance of switching the viewport in aid of the user friendliness however we plan on making this option available to developers where they decide if they would like to limit the number of viewport shuffles or not. Besides a desktop authentication system and a web based module we also plan on including support for mobile devices.

8. References

i. “Graphical Passwords: A Survey”, Xiaoyuan Suo Ying Zhu G. Scott. Owen, Georgia State University

ii. “Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice”, Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, Nasir Memon

iii. Arash Habibi, Lashkari, Farnaz Towhidi, Dr. Rosli Saleh, Samaneh Farmand, “A complete comparison on Pure and Cued Recall-Based Graphical User Authentication Algorithms” International Conference on Computer and Electrical Engineering, pp. 527-532, 2009.

iv. “Non-Functional Requirements: Do User Stories Really Help?”, Rachel Davies, Agile Experience Ltd, UK, <http://www.methodsandtools.com/archive/archive.php?id=113> Access Date: 20-April-2015

v. “PassPoints: Design and longitudinal evaluation of a graphical password system”, Susan Wiedenbecka, Jim Watersa, Jean-Camille Birgetb, Alex Brodskiyc, Nasir Memonc. - International Journal of Human-Computer Studies

vi. “Shoulder surfing defence for recall-based graphical passwords”, NH Zakaria, D Griffiths, S Brostoff, J Yan - Proceedings of the Seventh, 2011 - dl.acm.org

vii. “Graphical Password Authentication: Personalized Cued Click Points to overcome the limitations of Persuasive Cued Click Points.”, Victor Fernandes, Sweedal Lopes, Parima Gavaskar - The International Journal Of Science & Technoledge Sept 2014