Authentication Using Grid-Based Authentication Scheme and Graphical Password

Vijayshri D. Vaidya[1]
Department of Computer engineering
SND COE & RC
Yeola, India

Imaran R. Shaikh[2]
Department of Computer engineering
SND COE & RC
Yeola, India

Abstract: Currently the computer and internet become important part of everyone's life. The large amount of important data can be transferred as well as stored by the various applications. The user friendly applications are provided for easy handling. The various schemes are invented for securing such applications. Textual passwords as well as graphical passwords are used for authentication. But these authentication schemes are vulnerable to various types of attacks. Many times username is simple, so attacker can easily remember that and guess the password from it. So in proposed system we have developed two authentication schemes which provide the secret username as well as graphical password using cloud. The secret username is valid for that session only. After verification of secret username user can able to enter the graphical password. So, new scheme will provide the strong security using secret username in combination with graphical password.

Keywords—Authentication, graphical password, security, secret username, PCCP, cloud, session

I. INTRODUCTION

In the internet world, the computer has become the important part of everyone's life. There are many applications developed for easy handling by the different users. These applications are used to store these types of data and transferring the data. The areas like banking, e-commerce, business uses number of applications.

So to protect the applications, authentication techniques like textual passwords with various strengths are used. The vulnerabilities for textual passwords are dictionary attack, social engineering and shoulder surfing are well known. The passwords using combination of characters, symbols (i.e. random) and long passwords can provide the security to the system. But the main problem with these types of passwords is they are not easily remembered. Another authentication scheme is graphical passwords which are used for providing the high security.

In this paper, two new authentication schemes are proposed. These schemes authenticate the user by secret username [1] and graphical password. [2]

Every application needs the username and password for accessing it. Most of the time user uses the common usernames which are easily guessable by attacker. After getting the username the attacker can easily break the passwords by applying various techniques. Before providing the password for the application the secret username also be used for providing extra security in combination with passwords. Most of the attackers break the passwords by using clues related to usernames.

Authentication using password mainly contains two parts that are Knowledge based authentication and other is biometric authentication. Currently most of the web applications are using knowledge based authentication mechanism that provides the text passwords as well as graphical passwords. Many times the user can create the simple text passwords which are easily guessable or they can choose the complex which is not remembered by them easily. In e-world when we are having number of networks and personal accounts, some sort of easy authentication scheme is needed which can provide the best security.

In this paper securing cloud by using the knowledge based authentication using graphical password scheme is developed. The alphanumeric passwords are also used for cloud security but problem with the alphanumeric passwords is that they are not that much secure. The most important thing is that the user has to recall those passwords every time. The user has to give the higher priority for security for different accounts beyond their actual work. [6]

So to decrease the burden on user, the proposed system uses persuasive features in combination with cued-click-point for selecting the different images on click to create the graphical password.

The strong security can be provided by using secret username in combination with graphical passwords.

II. LITERATURE SURVEY

The previous work shows that there are no such schemes which provide the secret usernames.

No one consider that the username can also have a security.

Most of the schemes invented only for secure passwords. The common methods used are textual password or graphical password.

Some of them are follows:

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

A. Textual Passwords:

The textual passwords are easily guessable. The critical textual passwords are not easy to remember.[3] These passwords are vulnerable to different types of attacks.

B. Image based scheme:

Image-based scheme can uses the images including photo, artificial pictures, or other images at the background. Single image is provided to the user. The users have to select the particular points on that image.

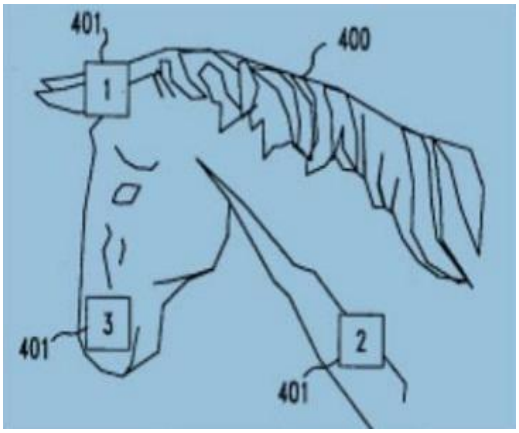

Figure-1.1: Single Image based scheme

The problem with this scheme is users have to pass through the number of selections on image and it takes more time.

C. Hybrid Authentication:

In this scheme, the user can rate the number for finding the particular sequence of colors and must remember the rating.

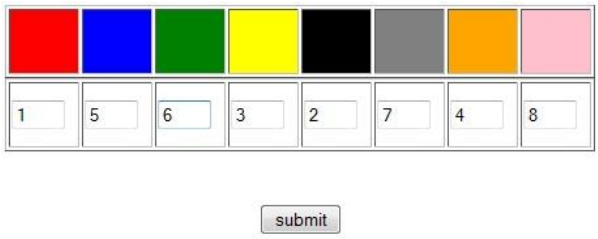

Figure-1.2: Hybrid authentication method

The problem with this scheme is to remember the colors with sequence.

D. Signature-Based Scheme:

In this scheme the signature of user is used as password.

Figure-1.3: Signature-based scheme

The problem with this scheme is to remember the grid of signature every time. If the grid is not remembered then user can't enter the password.

III. PROPOSED SYSTEM

In this paper we have developed two schemes which can provide the secret username and graphical password using cloud. Firstly the username can be authenticated and then user is able to enter the password. Authentication technique consists of 3 phases: registration phase, login phase and verification phase. During registration phase, user enters his username and the graphical password by fetching the images from cloud. During login phase, the user has to enter the username based on the grid-based interface displayed on the screen. The system verifies the username entered by comparing with content of the username generated during registration and then goes to password area. While providing the password user has to select the correct images and the correct click points on it. If both are correct then user is able to login.

A. Grid-Based Authentication scheme for secret username:

During registration user submits his username. Minimum length of the username is 4 and it can be called as secret username. The username should be of characters or numbers or combination of both. During the login phase, the user enters his secret username using the grid-based interface display. The grid is of size 6 x 6 and it consists of alphabets and numbers. The letters and digits are randomly placed on the grid and the interface changes every time. As the grid gets shuffle at every time, it prevents from the attacks like shoulder surfing.

Figure-1.4: Grid-Based Display

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

Figure shows the grid-based display in login interface. User has to enter the username depending upon the secret username. The secret username consists of characters or number or both.

Figure-1.5: Enter username using Grid-Based Display

Example: If the secret username is "**ABHI**"
In this username there are four letters as A**, B, H, I**.
While entering the secret username no need to enter real username. That means no need to enter the letters a, b, h, i. Instead of that, for letter **a** user has to find the letter in column and the letter in row whose intersection is letter **A**.
i.e. from grid user selects o (column) and 2 (row) whose intersection is **A**. Likewise user enters the secret username.

The secret username entered by the user is verified by the server to authenticate the user. If the username is correct, the user is allowed to enter the graphical password.

B. Selection of graphical password:

To create graphical password, user provided with five images. These images can be fetched from cloud and stored on the client machine temporarily. From given set of five images user has to select one click point on each image. Like this total five click points i.e. x, y coordinates of that click points are stored in the database as a password.

Persuasive Cued Click-Points:

PCCP [3] and CCP [4] are used in combination to encourage the users to select more random and strong passwords. It functions like CCP. During password creation the viewport positioning algorithm placed on the image and image can be divided into 4X4 grid. Then user has to select the favorite area and that area is the viewport area which is zoomed out to select the particular point. During the remaining parts of image gets blurred. Users select a click-point within this viewport (see fig 1.4), or press a "shuffle" to randomly reposition the viewport until a suitable location is found. On subsequent logins, images are displayed in their normal format with no blur or viewport. The design intent of the viewport is to pattern the distribution of click-points across multiple users, reducing hotspots and pattern formation.

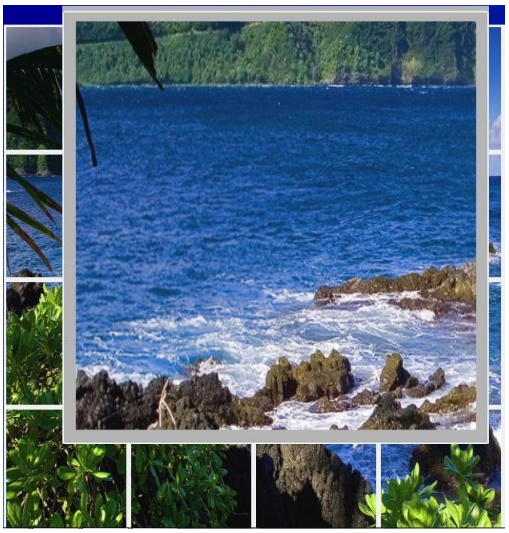

Figure-1.6: PCCP Viewport Detail

Different users might be select same images. Same images could be reused by two different users; highest probability of collision may be occurs. PCCP reportedly removes major concerns related to common patterns and hotspots. PCCP use a grid-based discretization [3] to find out whether login click-points are within that tolerance area. For verification, these passwords can be hashed; additional information such as a grid identifier (for each click-point), however, is stored in a manner accessible to the system, to allow the system to use the appropriate grid to verify login attempts.
At the registration time five images from cloud will be provided to the user. The user select the image and click on the image then next image will be open and process will continue till the password is created.
At login time if user selects the wrong click point on image then further wrong images can appear. The user will get acknowledgement of wrong password after final image click only.

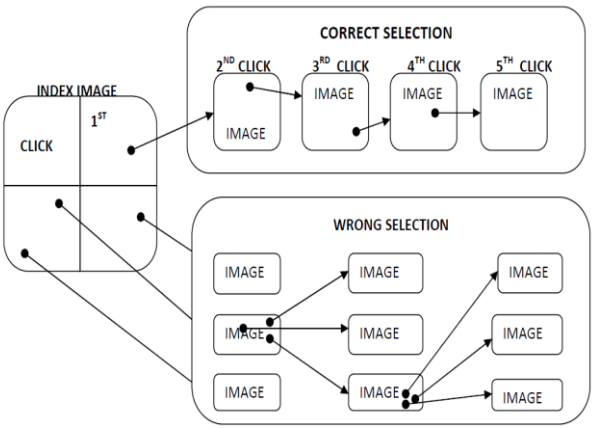

Figure-1.7: PCCP Image Selection Method

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

IV. RESULTS

The grid-based authentication scheme is used for secret username.

Table 1: Login time for entering the correct username

Technique	Avg	Min	Max
Grid-Based Authentication Scheme	26.25	18	40.30

The PCCP technique can be used as an algorithm for further authentication schemes.

As a security measure we have provided the authentication method in which admin will enter the username and password.

If that username and password both the fields are correct then only authentication will be successful. Else authentication will not be successful. Once this process successfully completes all other menus will be activated till then all menus will be kept hidden.

Fig. 1.8 : GUI for Administrator Login

In this GUI the administrator logs in and decides which password is given to the user for securing his application.

PCCP first image:

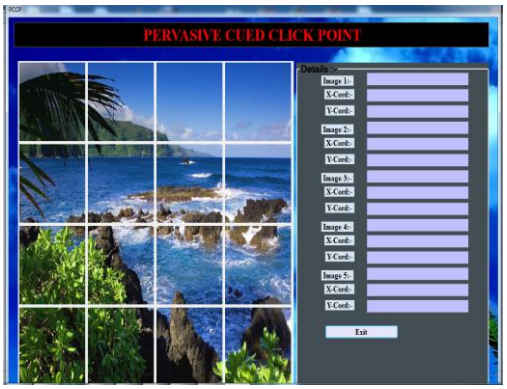

Fig. 1.9 : GUI for First Image of user

In this GUI the first image to be selected by the user in parts and the user needed to select the part and it is the basic front page of the authentication system.

PCCP Selection part:

Fig. 1.10 : GUI Display viewport of Image for selection

In this result the user select a part of the cropped image as authentication of the password selection that the user has to select first in order to exercise the results.

To make particular point selection on the part of image that part can be zoomed out. The part is called as viewport area.

The viewport area can provide the better visual to the user to select the most remembered part on the image as a click-point.

PCCP Coordinate selection part:

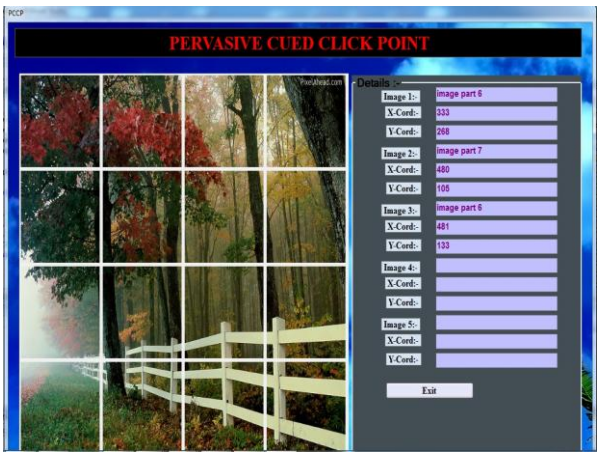

Fig. 1.11 : GUI-Coordinate Selection

In this GUI the user select a part of the cropped image as authentication of the password as first phase and then selects the coordinates of the zoomed result as the second phase which increases as the password progresses with each image thus gives a strengthened password.

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

PCCP Coordinate gets wrong while login:

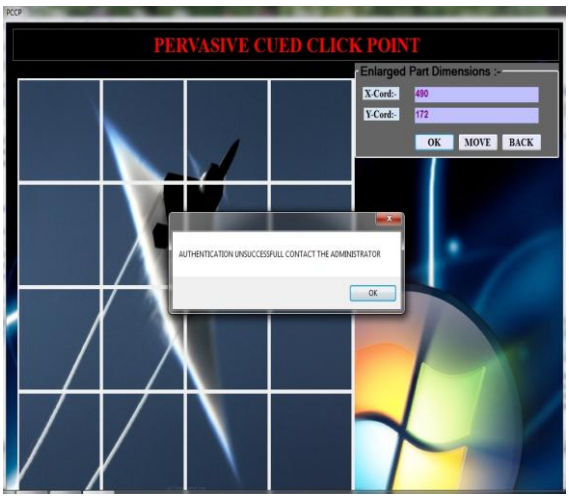

Fig. 1.12 : GUI-Wrong Selection

The GUI shows that if the user (attacker) selects the wrong click-points then authentication gets unsuccessful.

V. COMPARISON WITH OTHER METHODS

A. Grid-Based Authentication scheme for secret username:

The previous work shows that the pair-based scheme is used for password only. In the proposed system this scheme provides the secret username. So the scheme is the best option and has no comparison.

B. Graphical password:

Techniques	**Multiple Images used**	**Viewport Used**	**Strength of Password**
Pass Faces	No	No	4^2 **Low**
Single Image Based Scheme	No	Yes	4^2+100^{100} **Moderate**
KBAM	Yes	Yes	4^2+50^{50} X 12 **Good**
Proposed System	Yes	Yes	4^2+100^{100} X 5 **Better**

VI. ADVANTAGES

The secret username can provide the strong security with graphical password.

The secret username prevents from different attacks like eves dropping, dictionary attacks, social engineering and shoulder surfing.

Graphical password strongly resist the guessing attacks like pattern-based attacks, hotspot attack as well as capture attacks like shoulder surfing.

The graphical password created by the system is easy to remember and reliable as it uses the firewall of cloud.

The system uses free cloud and accesses the cloud servers.

The system can be accessed from anywhere.

The system can provide security to any application.

CONCLUSION

Thus secret username can be provided by grid-based scheme and graphical password authentication can be given by taking cloud as a platform. Both schemes are resistant to dictionary attack, brute force attack and shoulder-surfing .The proposed system solves the many problems of existing system. It can also be useful for user in security point of view as it provides the secret username and graphical password.

The proposed system will be used as an algorithm for further authentication schemes.

REFERENCES

[1] M Sreelatha, M Shashi, M Anirudh, MD Sultan Ahamer,V Manoj Kumar, "Authentication Schemes for Session Passwords using Color and Images", International Journal of Network Security & Its Applications (IJNSA),Vol.3, No.3,May2011.

[2] ShraddhaM. Gurav, Leena S. Gawade, Prathamey K. Rane, Nilesh R. Khochare, "Graphical password authentication cloud securing scheme" Computer Department, Mumbai University, RMCET Ratnagiri, India

[3] Sonia Chiasson, Member, IEEE, Elizabeth Stobert, Alain Forget, Robert Biddle, Member, IEEE, and P. C. van Oorschot, Member, "Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism" IEEE-2011

[4] Uma D. Yadav, Prakash S. Mohod "Adding Persuasive features in Graphical Password to increase the capacity of KBAM"Computer Science & Engineering G. H. R. I. E. T. W. Nagpur, India

[5] Farnaz Towhidi, "A Survey on Recognition-Based Graphical User Authentication Algorithms"Centre for Advanced Software Engineering, University Technology Malaysia Kuala Lumpur, Malaysia

[6] Susan Wiedenbeck Jim Waters, "Authentication Using Graphical Passwords: Basic Results" College of IST Drexel University Philadelphia, PA, 19104 USA

[7] G. Agarwal ,Deptt.of Computer Science, IIET, Bareilly, India Deptt. of Information Technology, IIET, "Security Analysis of Graphical Passwords over the Alphanumeric Passwords", India 27-11-2010

[8] Fabian Monrose, Michael K. Reiter, "Security Analysis of Graphical Passwords over the Alphanumeric Passwords"Networks J., vol. 4, no. 5, pp. 567-585, Sept. 2006.

[9] Susan Wiedenbeck, Jim Waters "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice"College of IST Drexel University Philadelphia

[10] Susan Wiedenbeck and Jim Waters "Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme"College of IST Drexel University Philadelphia, PA 19104 USA

[11] Sonia Chiasson, P.C. van Oorschot, and Robert Biddle, "Graphical Password Authentication Using Cued Click Points"ESORICS , LNCS 4734, p.359-374,Springer-Verlag Berlin Heidelberg 2007(IEEE oct. 2012)

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR