Strong Security Mechanism through Two Factor Authentication Text and Graphical Password

[1]Dr. Swapnaja Ubale, [2]Rekha Babar, [3]Pooja Bhise, [4]Shubham Nehere, [5]Tanuja Pawar
Department of Computer Engineering, ZCOER, Narhe, Maharashtra, India.

Abstract: *This paper presents an alternative visual authentication scheme with two secure layers for web-portals. Security mechanism like authentication and protection services is provided by passwords. According to human tendency, picture passwords are easy to remember then textual passwords. Hence this system provide two way authentication factor which is based on recognition and recall-based technique which is combination of graphical as well as text password that offers advantage over existing system and may be convenient for users. Shoulder surfing attack and many other attacks on graphical passwords are contrary to our scheme.*

Keywords: *Authentication, Cued Click Points, Graphical Passwords, Network Security, Shoulder Surfing, Server Side Images.*

I .INTRODUCTION

Computer Security contexts is important fundamental component were user authentication is necessary. It provides the support for access control and user liability [2]. Although there are many types of user authentication systems such as alphanumerical user name / passwords. They are functional and accessible to implement and handling.

To satisfy two contradictory requirements the alphanumerical passwords are required. They have to be easily remembered by a user, while they have to be hard to guess by con artist [3]. Users are familiar to choose easily guessable and brief text passwords, which are an easy target of dictionary and brute-forced attacks [4, 5, 6]. Accomplish a strong password policy sometimes leads to an opposite reaction, as a user may resort to write his or her difficult-to-remember passwords on sticky notes exposing them to direct theft.

In research, several techniques have been recommended to trim the limitations of alphanumerical password. One recommended solution is to use an easy to remember long phrases rather than a single word [7]. Another recommended solution is to use graphical passwords, in which graphics (images) are used rather than alphanumerical passwords [8]. This can be getting by asking the user to select field from an image instead of typing characters as in alphanumeric password approaches.

In this extended abstract, we recommended a two factor authentication system such as text and graphical password. The system combines text and graphical passwords trying to achieve the best of both worlds.

II. REALTED WORK

Graphical password based authentication systems are knowledge based system, which focuses on the fact that human can memorize and recognize images more easily than text password [1]. Graphical passwords are mainly classified into: recall based (draw metric) scheme- based on drawing or sketching shapes on screen, recognition based(econometric) scheme-based on selecting some known items from set of items and cued recall (loci metric)schemes-based on selecting regions of a known image.

III. PROJECT PROCESS AND TECHNIQUES

- **Recognition Base Techniques:**

  In these techniques some images are shown to the user during registration. The user has to select some images from the number of images. Afterwards as name indicates for valid login user has to recognize those preselected images in a correct sequence.

- **Recall Based Techniques:**

  In these techniques, user has to recall something that has been created or selected during registration. Recall-based password authentication are categorize in two parts:

  1) Pure Recall Based Technique:

  In this procedure, a user generates his password without giving any clue or reminder.

  2) Cued Recall Based Technique:

  In the cued recall based technique, the image cues the user. For example to click a set of option a set of point on an image means hint and reminder help

user to reproduce their passwords. Types of click based graphical password techniques:

Pass Points (PP):

In pass point the password is based on ordered sequence of three click-points on a pixel-based image. Pass Points (PP) is a click-based graphical password system. User must click within some system-defined tolerance region for each click-point at the time of login. Users remember their password click-points through image.

Cued Click Points (CCP):

CCP was developed as an alternative click based graphical password method where users select one point per image for three images. The interface displays only one image at a time; the image is replaced by the next image as soon as a user selects a click point. The click- point on the current image

The next image system determines the next image to on the user's display based displayed to users is based on a deterministic function of the point which is currently selected. It now presents a one to-one.

Cued recall scheme where each image activate the user's memory of the one click-point on that image. Secondly, if a user enters wrong click-point during login, the next image displayed will also be wrong. Users who see an unaware image know that they made an error with their previous click-point. Conversely, this unexpressed feedback is not helpful to an attacker who does not know the expected sequence of images.

The token can be combined with an orientation of image so that same image if presented at a different angle will not be able to authenticate the user. So not only the token but also the orientation of the token presented is important. In the second pass more precise extraction of frames from live video with accurate feature detection will be done. Selecting sequence of frames from thousands of frames will act as a password.

IV. MATHEMATICAL MODEL

Let S be the system,

Where S = {I, F, O, DD, NDD, Success, Failure| I= Input | F=function | O=Output |

DD=Deterministic Data| NDD=Non Deterministic Data}

NDD = {Search Input, Login}

DD = {User database}

Success:

1. Generation of destination profile for given destination name.

2. Generation of accurate User name and password for given destination.

3. Generation of suggested destinations**.**

V. SYSTEM ARCHITECHTURE

User registration process and User authentication process are shown in above system architecture. In User registration process user have to sign up and fill the information then first set the text password and then set the graphical password. To set graphical password user select pass point in multiple images. In User authentication process user login with user id and enter the text password if text password is correct then select pass points of images for graphical password. Verification of user id and password from database if image selection is wrong then authentication failed if image selection is correct then authentication successful.

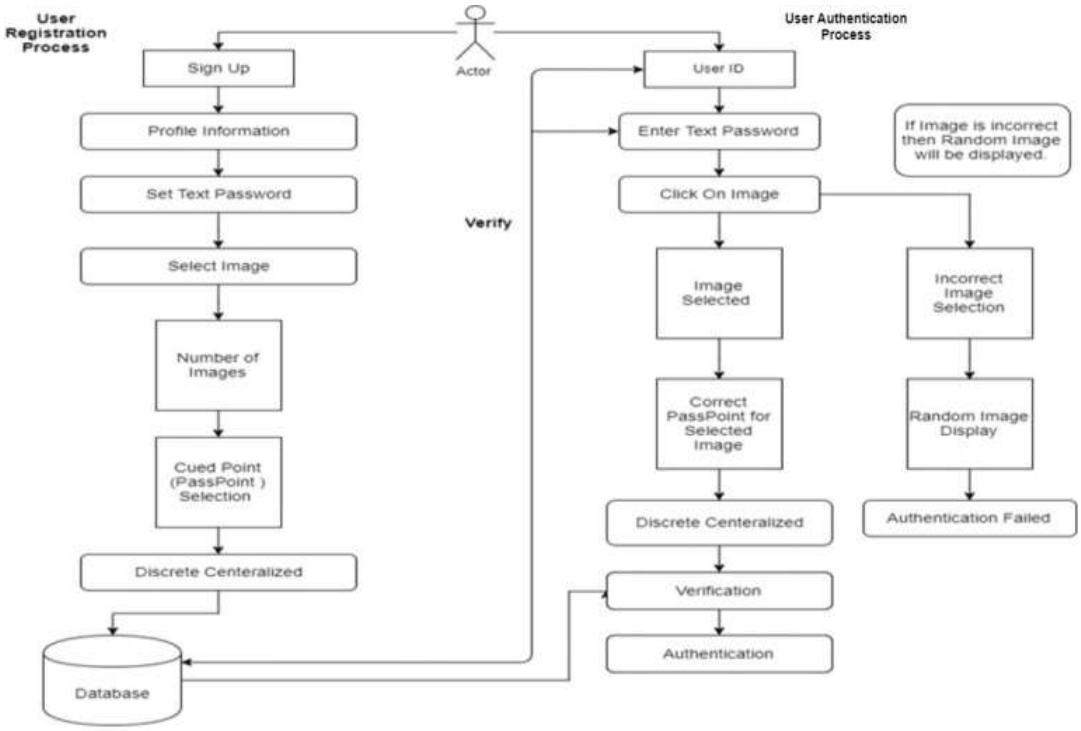

Fig.1.System Architecture

VI. CONCLUSION

Proposed System is improving the security of password by two factor authentications like text password and integrating images. Two factor authentications substantially increases protection to shoulder-surfing attacks compared with existing graphical password schemes. Providing Strong Security through two factor authentication tackles this problem by introducing a physical token into the authentication process. This way, a two factor authentication traditionally to a more secure multifactor authentication method.

REFERENCES

[1] Andrea Bianchi, Ian Oakley, and Hyoungshick Kim," PassBYOP: Bring Your Own Picture for Securing Graphical Passwords" 2168-2291 © 2016 IEEE.

[2] William Stallings and Lawrie Brown. Computer Security: Principle and Practices. Pearson Education, 2008.

[3] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget,Alex Brodskiy, and Nasir Memon. Pass points: designand longitudinal evaluation of a graphical password system. International Journal of Human-ComputerStudies, 63:102–127, July 2005.

[4] Robert Morris and Ken Thompson. Password security a case history. Communications of the ACM, 22:594–597, November 1979.

[5] Daniel V. Klein. Foiling the Cracker: A Survey of and Improvements to, Password Security. the 2nd USENIX UNIX Security Workshop, 1990.

[6] Eugene H. Spafford. Observing reusable password choices. In Proceedings of the 3rd Security Symposium. Usenix, pages 299–312, 1992.

[7] Sigmund N. Porter. A password extension for improved human factors. Computers & Security, 1(1):54– 56, 1982.

[8] Xiaoyuan Suo, Ying Zhu, and G. Scott Owen. Graphical passwords: A survey. In Proceedings of Annual Computer Security Applications Conference, pages463–472, 2.

[9] S.A. Ubale, "Comparison of ACL Based Security Models for securing resources for Windows operating system", International Journal Of Software and Hardware Research in Engineering, ISSN No. 2347-4890 Volume 2 Issue 6, June 2014.

[10] S.A.Ubale, "Bio-enable Security for Operating System by Customizing Gina, High Performance Architecture and Grid Computing" , Volume 169 of the series Communications in Computer and Information Science pp 179-185, Springer Berlin Heidelberg.

[11] Ubale S. A, Apte Sulabha ," Analysis of DAC MAC RBAC Access Control based Models for Security", International Journal of Computer Applications, Volume 104 No.5, October 2014.