JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Graphical Password Authentication System by Using Pass Point Scheme

1st Vinitha. V M. Sc., 2nd Mrs. S.KALAISELVI M.C.A., M.Phil., B.Ed , 3rd BHUVANESWARI R, M. Sc., M. Phil., M. Tech., SET

PG Student in computer science D.K.M college for women(Autonomus)

Assistant professor in computer science and application.
D.K.M. College for women(Autonomus)
Vellore
Assistant Professor in Computer science and Applications,D.K.M. college for women (Autonomous), Vellore

ABSTRACT

Authentication is the first line of defence against compromising confidentiality and integrity. Alphanumerical usernames and passwords are the most common method of computer authentication. This method has many drawbacks. Usually people use passwords that can be easily guessed, so that it does not becomes hard to remember. Hence to encounter this problem, researchers have developed graphical password authentication methods that use pictures as passwords. Graphical passwords are an alternative to text-based passwords where user is asked to recall an image or parts of an image instead of a word. We are further discussing new and more secure graphical password system called pass points. In pass points system users can create many points click sequence on a background image. The graphical password is new technique which is more secure than text-based passwords. In graphical passwords, sequence of clicks is generated to derive the password. The click events are performed on same image or different image. Or users can also select sequence of images. In this system there are four main modules namely, Image submission, Image Password Point Mark, Pixel Tolerance Calculation and Authentication. Users can submit image then he/she can click on the image to create a password then the system pixel tolerance calculates each pixel around. And then while authenticating user needs to click within the tolerances in the correct sequences.

1. INTRODUCTION

During early days text password was the well-known and only proposed computer authentication scheme to authenticate the user. Initially text passwords were used for authentication system. Text password is nothing but simply collection of characters or string. As how user has to always create their own passwords for different systems, which would be remember able but hard to guess attackers. But text passwords are easy to hack with some hacking techniques like brute force and fishing attacks. As well as it is again difficult to remember more than one text password for number of different systems to the user. After some time, biometric and token based password authentication systems were introduced as an alternatives to the text password but again it has its own drawbacks as it requires extra hardware setup and cost to setup new system for it. After some time, as alternatives for all those methods introduced is graphical password authentication system as it is very cheap and best. As well as per psychological studies user can remember graphical passwords very well than text passwords. Graphical password is of three types: Click based graphical password scheme, Choice based

graphical password scheme, Draw based graphical password scheme. In this paper proposed here, user clicks on single point of five images coming one after one in random sequence. User has to click five points on five images at the time of login process. While register user sets five click points to pass during login process. While registering user sets five images from image pool or from local drive. Based on image selection system generates the new signature. While user come to login phase he has to select the point over the image then system again generates the new signature for that point and if both signatures are same then and then user can be said ad authenticated user. Otherwise system will go in finite loop and show multiple wrong images to click. In mid of these images system inserts the right image to give one more chance to authenticate the user.

2. LITERATURE SURVEY

Title: The design and analysis of graphical passwords
Author: Ian Jermyn, Alain Mayer
Year: 1999
Description: In this paper we propose and evaluate new graphical password schemes that exploit features of graphical input displays to achieve better security than text-based passwords. Graphical input devices enable the user to decouple the position of inputs from the temporal order in which those inputs occur, and we show that this decoupling can be used to generate password schemes with substantially larger (memorable) password spaces. In order to evaluate the security of one of our schemes, we devise a novel way to capture a subset of the "memorable" passwords that, we believe, is itself a contribution. In this work we are primarily motivated by devices such as personal digital assistants (PDAs) that offer graphical input capabilities via a stylus, and we describe our prototype implementation of one of our password schemes on such a PDA, namely the Palm Pilot™.

Title: Security of Biometric Authentication Systems
Author: Vashek Matyas, Zdenek Riha

Year: 2010

Description: This overview paper outlines our views of actual security of biometric authentication and encryption systems. The attractiveness of some novel approaches like cryptographic key generation from biometric data is in some respect understandable, yet so far has lead to various shortcuts and compromises on security. Our paper starts with an introductory section that is followed by a section about variability of biometric characteristics, with a particular attention paid to biometrics used in large systems. The following sections then discuss the potential for biometric authentication systems, and for the use of biometrics in support of cryptographic applications as they are typically used in computer systems.

Title: Cued Click Point Technique for Graphical Password Authentication

Author: Vaibhav Moraskar1, Sagar Jaikalyani2

Year: 2014

Description: In today's world the password security is very important. For password protection various techniques are available. Cued Click Points are a click-based graphical password scheme, a cued-recall graphical password technique. Users Click on one point per image for a sequence of images. The next image is based on the previous click-point. The passwords which are easy to memorize are chosen by the users and it becomes easy for attackers to guess it, but the passwords assigned by the strong system are difficult for users to remember. In this paper, we focus on the evaluation of graphical password authentication system using Cued Click Points, including usability and security. In this authentication system, our usability goal is to support the users in selecting better passwords, thus increases the security by expanding the effective password space. The emergence of hotspots is mainly because of poorly chosen passwords. Thus click-based graphical passwords encourage users to select more random, and hence more complex to guess, click-points.

3. PROPOSED SYSTEM

In pass points system users can create many points click sequence on a background image. The graphical

password is new technique which is more secure than text-based passwords. In graphical passwords, sequence of clicks is generated to derive the password. The click events are performed on same image or different image. Or users can also select sequence of images. In this system there are four main modules namely, Image submission, Image Password Point Mark, Pixel Tolerance Calculation and Authentication. Users can submit image then he/she can click on the image to create a password then the system pixel tolerance calculates each pixel around. And then while authenticating user needs to click within the tolerances in the correct sequences.

4. MODULES

The system comprises of 4 major modules as follows:

- **Image Submission:**
  - User can submit image.
- **Image Password Point Mark:**
  - User click on an image to create a password.
- **Pixel Tolerance Calculation:**
  - A tolerance around each chosen pixel is calculated.
- **Authentication**:
  - For authentication, user must click within the tolerances in the correct sequences.

5. CONCLUSION

The proposed Cued Click Points scheme shows promise as a usable and memorable authentication mechanism. By taking advantage of users' ability to recognize images and the memory trigger associated with seeing a new image, CCP has advantages over Pass Points in terms of usability. Being cued as each images shown and having to remember only one click-point per image appears easier than having to remember an ordered series of clicks on one image. CCP offers a more secure alternative to Pass Points. CCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then conduct hotspot analysis on each of these images. In future development we can also add challenge response interaction. In challenge response interactions, server will present a challenge to the client and the client need to give response according to the condition given. If the response is correct then access is granted. Also we can limit the number a user can enter the wrong password.

6. RESULT

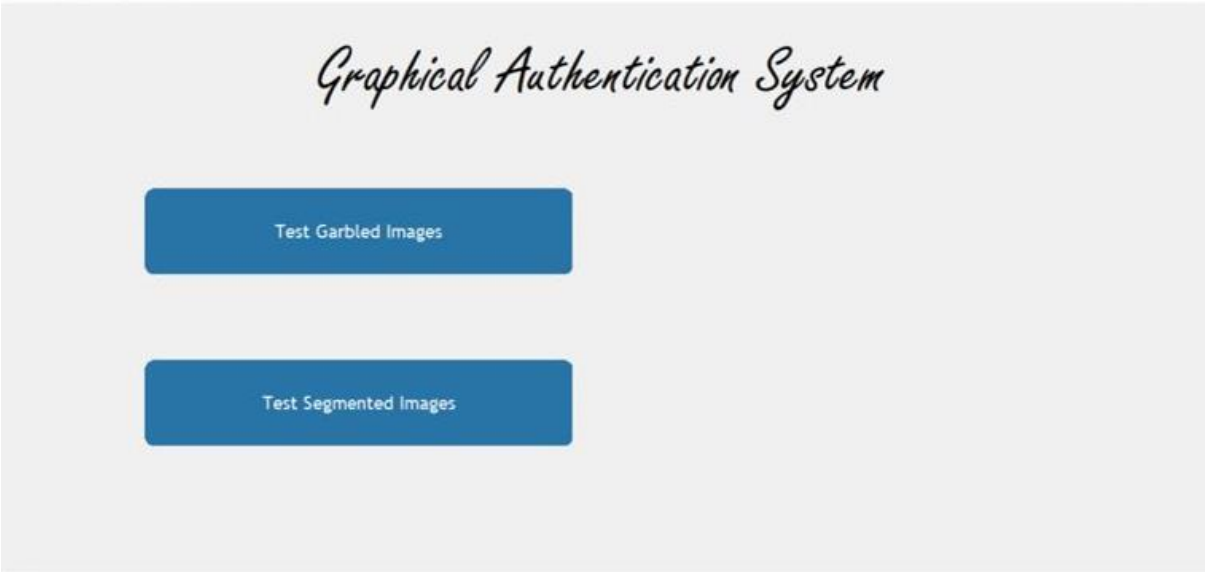

Fig 1: login Screen

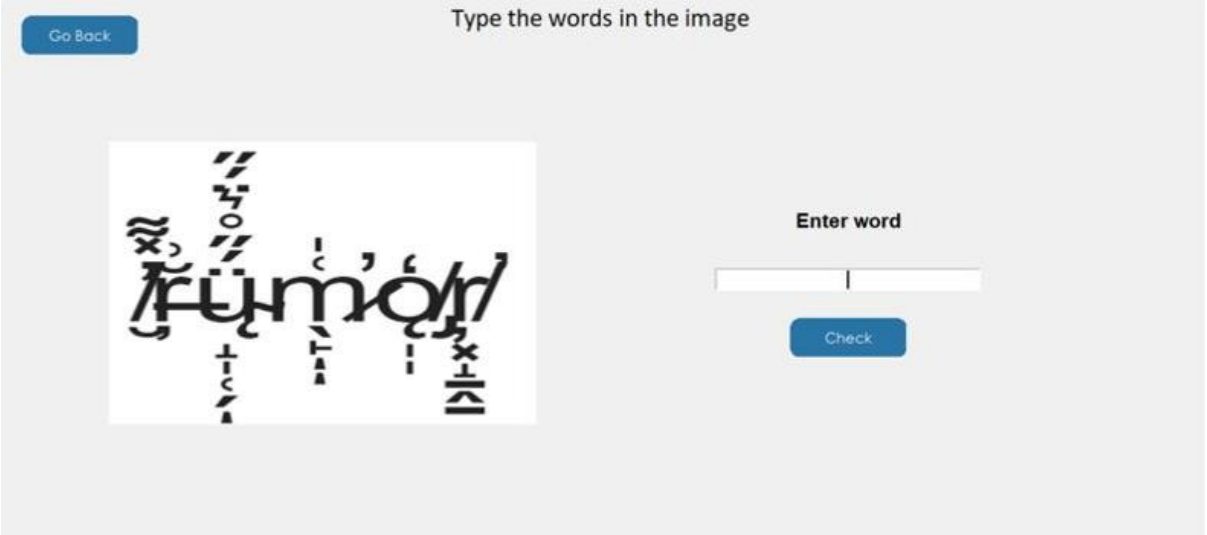

Fig 2: Validation Screen

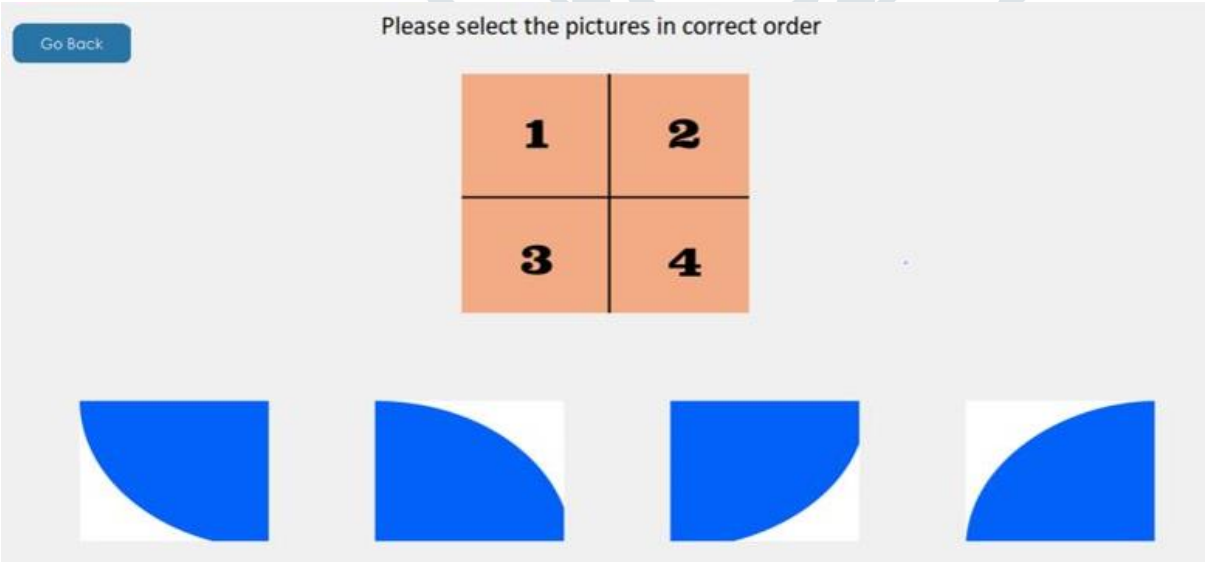

Fig 3: Graphical Authentication

7. FUTURE SCOPE

In future it has great scope. It can be used everywhere instead of text-based password .We can increase the security of this system by increasing the number of levels used, the number of tolerance squares used. Presently there are many authentication system but they have their own advantages and disadvantages. Text password can

be hacked easily with various methods where as biometric authentication can cause more cost.

8. REFERENCE

[1] “The Design And Analysis Of Graphical Passwords”, Ian Jermyn, Alain Mayer, Fabin Monrose, Michael K. Reither, Aviel D. Rubin, Proceeding of The 8th UNISEX Security Symposium, 1999

[2] “Security of Biometric Authentication System”, Vashek Mathyas, Zdenek Riha, International Journal of Computer Information System And Industrial Management Application, 2011

[3] “Graphical Password Authentication Using Peruasive Cued Click Point”, Iranna A. M., Pankaja Patil, International Journal Advanced Research in Electrical Instrumentation Engineering, Julay 2013.

[4] “Graphical Passwords: A Survey”, Xiaoyuan Suo, Ying Zhu, G. Scott.Owen, (Department of Computer Scince Georgia State University).

[5] “Persuasive Cued Click Points With Click Draw Based Graphical Password Scheme”, P. R. Davele Shrikala M. Deshmukh, Anil B. Pawar., International Journal of Soft Computing and Engineering (IJSCE), May 2013.