ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A SECURE WAY OF LOGIN WITH PERSUASIVE CUED CLICK POINTS AND PASSFACES

Preeti
Department of ISE
BMS College of Engineering

ABSTRACT

Text passwords are the most prevalent user authentication method, but have security and usability problems. Replacements such as biometric systems and tokens have their own drawbacks. Graphical passwords offer another alternative. The main issues of knowledge-based authentication, usually text-based passwords, are well known. Users tend to choose memorable passwords that are easy for attackers to guess, but strong system assigned passwords are difficult for users to remember. An important usability goal for authentication systems is to support users in selecting better passwords, thus increasing security by expanding the effective password space.

Keywords: ***authentication; usability, security, graphical passwords, memorable***

INTRODUCTION

Today, authentication is the principal method to guarantee information security and the most common and convenient method is password authentication.Traditional alphanumeric passwords are strings of letters and digits, which are easy and familiar to all users. However, there are several inherent defects and deficiencies in alphanumeric passwords, which easily evolve into security issues. Due to the limitation of human memory, most users tend to choose short or simple passwords which are easy to remember. Surveys show that frequent passwords are personal names of family members, birth date, or dictionary words. In most cases, these passwords are easy to guess and vulnerable to dictionary attack .Today users have many passwords for personal computers, social networks, E-mail, and more. They may decide to use one password for all systems to decrease the memory burden, which reduces security. Moreover, alphanumeric passwords are vulnerable to shoulder surfing attack, spyware attack and social engineering attack etc. Motivated by the promise of improved password usability and security, the concept of graphical passwords was proposed in 1996 [1].

Like alphanumeric passwords, graphical passwords are knowledge-based authentication mechanisms. The main goal of graphical passwords is to use images or shapes to replace text, since numerous cognitive and psychological studies demonstrated that people perform far better when remembering pictures than words. The most widely accepted theory explaining this difference is the dual-coding theory suggesting that verbal and non-verbal memories are processed and represented differently in the mind. Assigned with perceived meaning based on direct observation, the images are represented in a way that retains the perceptual features being observed. The text is represented with symbols that convey associatively cognitive meaning. As a result, additional processing required for verbal memory renders a more difficult cognitive task. Thus it is easy for human being to remember faces of people, places they visit. etc. There are a plenty of papers on graphical passwords, some of which focus on specific schemes while others focus on concrete attacks.

BACKGROUND STUDY

Current authentication methods can be divided into three main Categories [5]:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number.

Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

approach is that such systems are expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security.

- Recognition-based graphical techniques
- Recall-based graphical techniques

In recognition-based techniques, a user is challenged with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage.

In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

Earlier several graphical Password techniques were introduced. Some of the techniques are given below:

Persuasive Cued Click Points (PCCP)[2]:

For creating Persuasive Cued Click Points persuasive feature is added to CCP [2] .PCCP encourages users to select less predictable passwords. For password creation PCCP uses terms like viewport & shuffle. When users creating a password, the images are slightly shaded except for a viewport as to avoid known hotspots the viewport is positioned randomly. The most useful advantage of PCCP is attackers have to improve their guesses. Users have to select a click-point within the highlighted viewport and cannot click outside of the viewport unless they press the shuffle button to randomly reposition the viewport. Only at the time of password creation, the viewport & shuffle button appears. After the password creation process images displayed normally without the viewport & shuffle button.

Fig 1. Password creation in PCCP. Highlighted area is viewport

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture based passwords. The picture-based techniques can be further divided into two :

Passface [4] is a technique developed by Real User Corporation. In this, the user will be asked to choose four images of human faces from a face database as their future password. In the authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces. The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies the four faces. The technique is based on the assumption that people can recall human faces easier than other pictures.

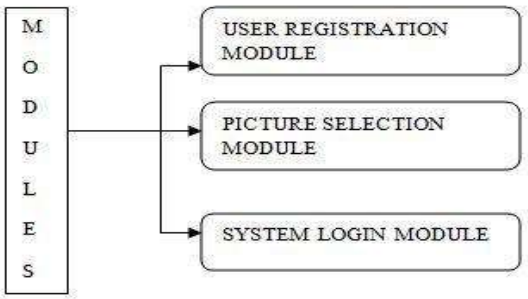
Fig 2. An example of Passfaces

PROPOSED SYSTEM

My proposed system consists of following things:

A. System Design

The system design consists of three modules such as user registration module, picture selection module and system login module [3].



ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Fig 3. System design modules

In user registration module user enters the user name in user name field and also suitable tolerance value (tolerance value is use to compare registration profile of user with login profile of the same user). When user entered the all user details in registration phase, these user registration data will get stored in data base and used during login phase for verification.

In picture selection phase there are two ways for selecting picture for password authentication.

1. User defines pictures: Pictures are selected by the user from the hard disk or any other image supported devices.
2. System defines pictures: pictures are selected by the user from the database of the password system.

In picture selection phase ,there are two phases which are described below:

1st phase: User need to select one image as passwords and consist of a sequence of five click-points on that given image. Users may select any pixels in the image as click-points for their password. During the password creation,most of the part of image is dimmed except for a small viewport area that is randomly positioned on the image. Users must select a click-point within that viewport only. If they are unable or unwilling to select a point in the current viewport, they may press the Shuffle button to randomly reposition the viewport. The viewport guides users to select more random passwords that are less likely to include hotspots.During system login, the images are displayed normally, without shading or the viewport, and repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points.

2nd phase: In this phase user is asked to select four human faces in a sequence from the database provided by the system.

1) User Registration Flow Chart

The following flowchart shows the user registration procedure, this procedure include both registration phase (user ID) and picture selection phase. The process flow starts from registering user id and tolerance value. Once user finishes all the user details and then proceed to next stage, which is selecting click points on generated image,which will be five in number. After that user will select the four human faces from the database.When this procedure gets over, user profile will be created.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA) Impact Factor: 2.114

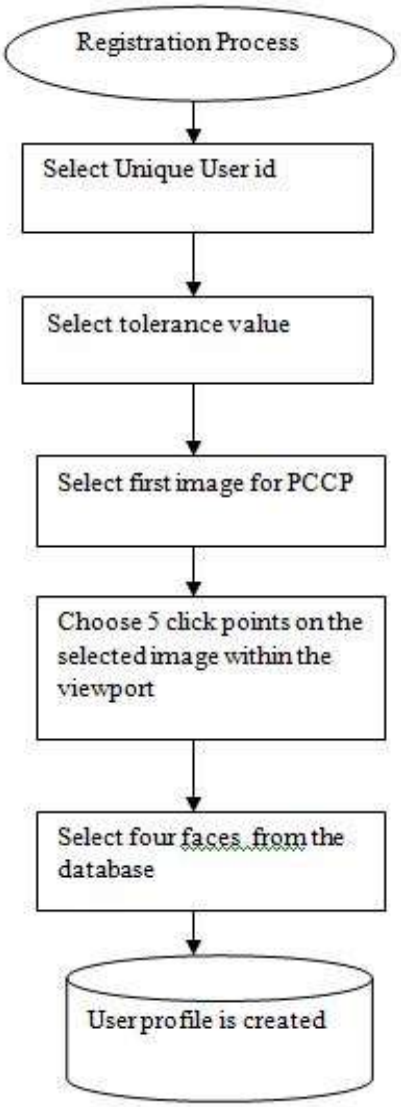


Fig 4. User Registration Flow Chart

2) *Login Procedure*

In this login procedure,first user enters the unique user ID as same as entered during registration.Then images are displayed normally, without shading or the viewport, and user need to repeat the sequence of clicks in the correct order, within the same tolerance as selected in the registration phase and then the user will be challenged with the grid containing nine faces from which user has to select one face and other eight faces will be decoy faces.This will go upto three more rounds until the user selects all the four faces.After finishing this procedure, user profile will be opened.

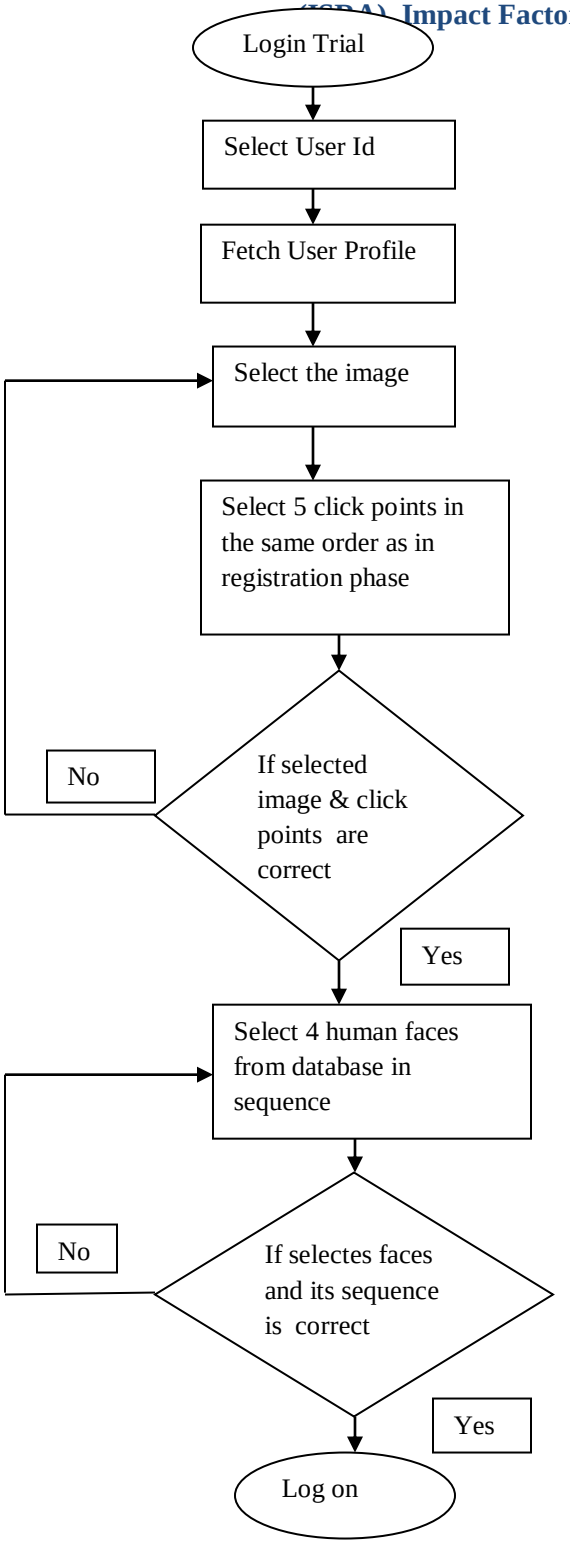


Fig 5. User login flow chart

CONCLUSION

My proposed scheme has various advantages such as it will be hard for attackers to

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

guess the password because using feature of PCCP patterm formation attacks and HOTSPOTS will be removed using viewport & shuffle button.Shoulder surfing is also not possible because in PCCP,the viewport will be randomly positioned everytime the new user will create a password in the registration phase. My system provides both features of graphical password authentication technique i.e, hard to guess using PCCP and easy to remember using Passfaces.Due to PCCP higher security is achieved and with the introduction of the passfaces less time will be required to create a strong password as human faces are easy to recall rather than other pictures.

REFERENCES

[1] Mohammad Sarosh Umar and Mohammad Qasim Rafiq. "Select-to-Spawn: A Novel Recognition-based Graphical User Authentication Scheme",2012 IEEE,ICCET.

[2] P. R. Devale Shrikala M. Deshmukh, Anil B.Pawar." Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013.

[3] Iranna A M ,Pankaja Patil."Graphical Password Authentication Using persuasive Cued Click Point", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, July 2013.

[4] Samir Kumar Bandyopadhyay, Debnath Bhattacharyya PoulamiDas. "User Authentication by Secured Graphical Password Implementation",2008 IEICE.

[5] Farnaz Towhidi, Arash Habibi Lashkari, DR. Rosli Saleh, Samaneh Farmand."A Complete Comparison On Pure And Cued Recall-Based Graphical User Authentication Algorithms",2009 Second International Conference on Computer and Electrical Engineering.

[6] Alireza Pirayesh Sabzevar, Angelos Stavrou "Universal Multi-Factor Authentication Using Graphical Passwords",2008 IEEE International Conference on Signal Image Technology and Internet Based Systems