Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

SHOULDER SURFING RESISTANT GRAPHICAL PASSWORD

Kruthi K[1], Kumuda B G[2], Nandhini N V[3],
Mrs. R.Anitha[4] (Associate Professor)
[1, 2, 3, 4]*Department of Computer Science and Engineering,*
The National Institute of Engineering, Autonomous under VTU
Mysore – 570008, Karnataka, India

Abstract— Shoulder surfing resistant graphical password system features a graphical password systems in a challenge-response scheme.This system is resilient against shoulder surfing attacks. When users input their passwords in a public place, they may be at risk of attackers stealing their password. An attacker can capture a password by direct observation or by electronic capture or by video recording the individual's authentication session. This is referred to as shoulder-surfing and is a known risk, of special concern when authenticating in public places. This system makes use of the convex hull click (CHC) scheme to prevent shoulder surfing.User can also go for second phase of verification, where a one time password (OTP) is generated and is sent to the user via email or message. This application allows the user to use their password safely in an insecure location.

Keywords-Shoulder-surfing, Convex Hull Click , graphical passwords, one time password, authentication.

I. INTRODUCTION

Shoulder surfing resistant graphical password is a project which features a graphical password systems in a challenge-response scheme. Shoulder surfing refers to someone watching over the user's shoulder as the user enters a password, thereby capturing the password. In a challenge-response scheme the user creates a password by choosing several images from a large portfolio of images. The chosen images become the user's password. To log in, the user must successfully respond to a series of challenges. In a challenge the user is simultaneously shown several images on the screen, where one of the images is a password image of the user and the rest are decoy images. The user responds by clicking anywhere on the password image. In each subsequent challenge the user is shown another password image surrounded by different decoys. The user logs in successfully if all challenges are responded to correctly.

The advantage of this kind of challenge-response system relies on recognition memory. In each challenge the user simply views displayed images and chooses the known image.A larger password space, and therefore higher security, can be achieved only by a large number of decoy images in each challenge or a large number of challenges. Both of these increase the login time.
Usability testing of the Convex Hull Click(CHC) scheme showed that novice users were able to enter their graphical password accurately and to remember it over time. However, the protection against shoulder-surfing comes at the price of longer time to carry out the authentication.

II. EXISTING SYSTEM

Traditionally, alphanumeric passwords have been used for user authentication. In this scheme ,the user has to enter the alphanumeric characters to login .This is a memory based scheme and it is difficult for humans to remember random strings. So,the users tend to keep the password small and simple. Thus they ignore requirements for secure passwords.

Smart card and biometric authentication scheme requires an external device for authentication. It is expensive when compared to other authentication techniques and if the smart card is misplaced ,there are chances of unauthorized access.

In an effort to improve password security by making passwords easier to remember, researchers have developed graphical passwords. In graphical password method,the user has to select a set of pass-icons from a pool of icons at the time of registration. To login the user has to select the same set of pass-icons. Users' memory for a graphical password may be better than for an alphanumeric password. Secure alphanumeric passwords (i.e., random strings) are based on pure recall from memory, a skill that is notoriously difficult for humans.

By contrast, graphical passwords are based on recognition of previously known images, a skill at which humans are proficient. But this method does not provide protection against shoulder surfing. Someone watching over the user's shoulder can easily capture the pass-icons.

III. PROPOSED SYSTEM

A. Avantages Of The Proposed System

- It is difficult to break graphical passwords using traditional attack methods such as :Brute force search,Dictionary Attack .
- Protects against shoulder surfing.
- The entered password is unique everytime.
- Easier to memorize when compared to alphanumeric passwords.
- It is difficult to track mouse clicks using spyware and thus protects against spyware attack.

B. Convex Hull Click Scheme

In this application we make use of Convex Hull Click (CHC) scheme to make the application resilient to shoulder surfing attacks.The Convex Hull Click (CHC) scheme provides several icons or images are randomly distributed on the screen.The system uses a large portfolio consisting of several hundred icons. In a challenge the user must recognize his or her password icons, or pass-icons, out of a much larger number of randomly arranged icons. To login the user should click on all the icons within the convex hull of the pass-icons.The convex hull of a set of points is the smallest convex polygon containing the points. A convex polygon is a nonintersecting polygon whose internal angles are all convex (i.e., less than 180 degrees). Several such challenges are presented in sequence, and if the user responds correctly to everyone then the user is authenticated.

To create a password the user chooses several icons from the portfolio to be his or her pass-icons (Figure 1). The number of pass-icons is determined by the system administrator. The user has to remember the pass-icons he or she selected.

Figure 1.Select Pass- icons

At login time a large number of icons are displayed randomly in the password window (Figure 2). These icons include mostly non-pass-icons along with a few pass-icons.

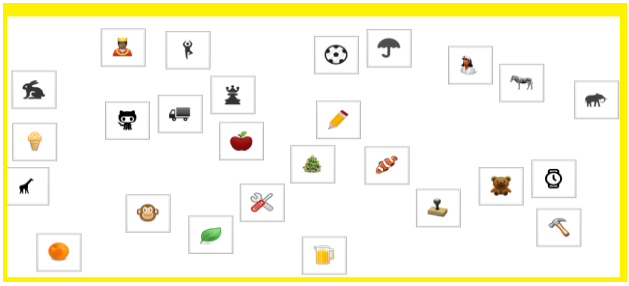

Figure 2. Randomly Distributed Icons

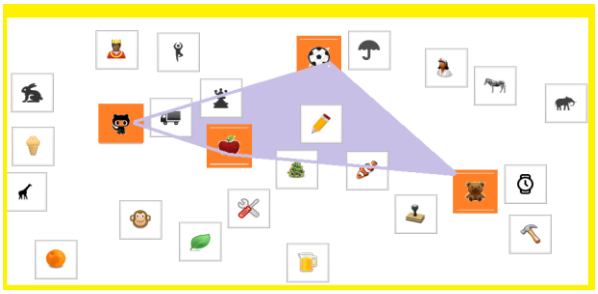

Figure 3.Virtual Convex Hull

At the time of login , the user must visually locate his or her pass-icons. The user's next step is to mentally create the convex hull formed by those pass-icons.For illustrative purposes, Figure 3 shows a highlighted convex hull formed by the pass- icons. To login succesfully the user must click all the icons present within the convex hull. If the user has chosen second phase of authentication ,then a One Time password is generated and is sent to the user via email or message.The login processs will successful only if the user enters the correct One Time password.

C. U*sability Of CHC*

It can be used for novices and expert both, novices could learn, remember, and enter passwords successfully using CHC. As no of total icons increased the time of login increased and as no of password icons increases time of login decreases because it is easier to find convex hull with grater no of icons. According to a survey conducted mean time of login with three password icon is found to be 11.72 sec, with four icons is 11.55 and with five icons is 9.71 sec for five roudnd. All the user were able to enter the password correctly in all 10 attempts. It was found that more the user will practice the more the login time will be decreased.So,It was advised that user should practice it for quick login. It is Secure to Brute force attack beacause of large no of icons and stages and it is secure to shoulder surfing attack.

No of Icons	Mean Time	Std Deviation
3	11.72	3.77
4	11.55	4.74
5	9.71	3.82

Table 1. Means and standard deviations (seconds) of challenges with 3, 4, and 5 pass- icons

IV. SYSTEM ARCHITECTURE

A. Presentation tier

This is the topmost level of the application. The presentation tier displays information related to such services as browsing merchandise, purchasing and shopping cart contents. It is a layer which users can access directly such as a web page, or an operating systems GUI. In this application this tier includes the user details entered such as username, user E-mail id, phone number e.t.c. The user will enter his username and password for the authentication.

B. Application tier

The logical tier is pulled out from the presentation tier and, as its own layer; it controls an application's functionality by performing detailed processing. In this user data will be accepted and processed. Convex hull click algorithm is used to confirm the user data correctness. This tier examines the user password and compares it with the database and returns the result to the user.

C. Data tier

The data tier includes the data persistence mechanisms (database servers, file shares, etc.) and the data access layer that encapsulates the persistence mechanisms and exposes the data. The data access layer should provide an Application Programming Interface (API) to the application tier that exposes methods of managing the stored data without exposing or creating dependencies on the data storage mechanisms. The database stores the user information with the passwords.

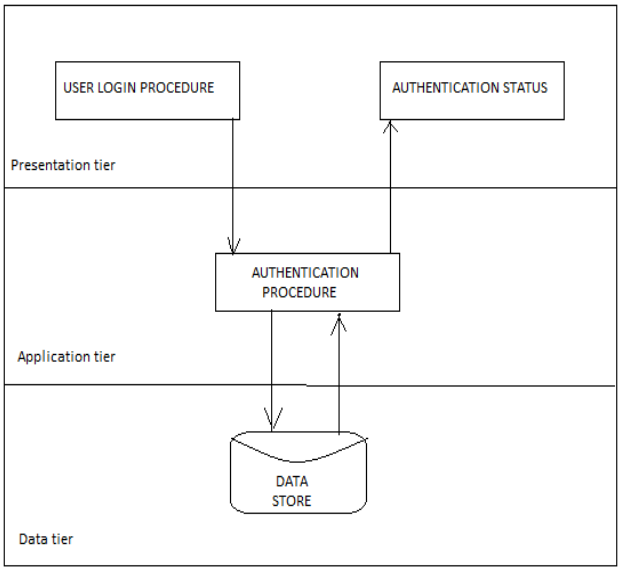

Figure 4. System Architecture

V. DATA FLOW DIAGRAM

.

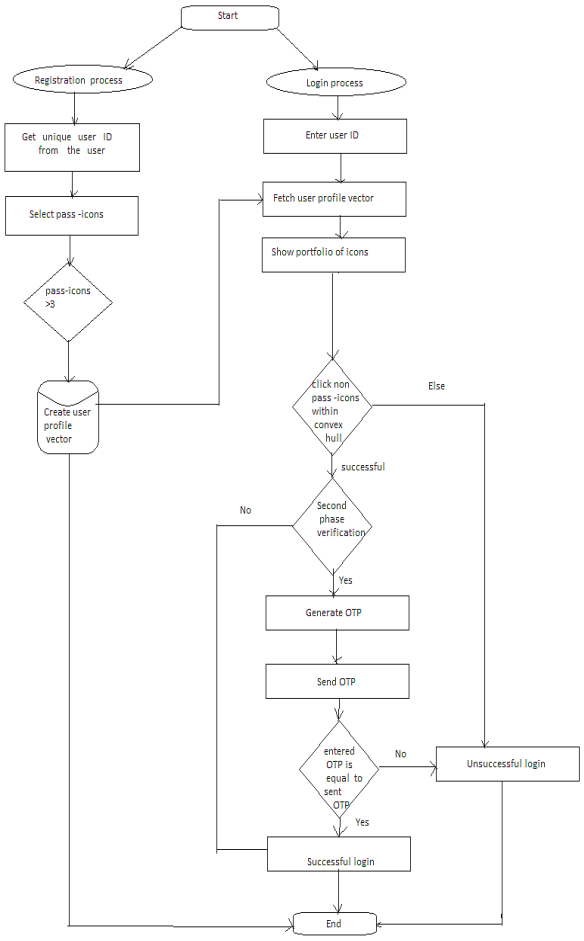

Figure 5. Data Flow Diagram

VI. APPLICATIONS

- Can be applied to web log -in application.
- Can be applied to workstations, ATM machines and mobile devices.

VII. CONCLUSION

The Convex Hull Click Scheme is an effort to develop security innovations with people in mind. As such, it is an example of "usable security," an approach to design of security systems that is gaining increasing attention. The contribution of this project is the design of a graphical password system that extends the challenge- response paradigm to resist shoulder-surfing. In doing so, it aims to motivate the user with a fun, game-like visual environment designed to develop positive user effect and counterbalance the drawback of the longer time to input the password.

REFERENCES

1. Software Engineering: A practitioner's approach, 6th Edition, Tata McGraw-Hill Edition 2010, by Roger S Pressman.
2. The complete reference VB .Net , Third Edition, Tata McGraw-Hill Edition 2006, by Naughton Schildt.
3. A paper presented in International Journal of communication and engineering on 01 March 2012 entitled Defenses Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points"
4. IEEE paper "Design and evaluation of a shoulder-surfing resistant graphical password scheme" submitted by Susan Wiedenbeck and Jim Waters and Leonardo Sobrado and Jean-Camille Birget De Angeli, A., Coutts, M., Coventry, L., Cameron, D.
5. http://www.w3schools.com/