

Shoulder-Surfing Resistant Graphical Password System

Deepak Vishwakarma¹, Rushikesh Nikumbe², Manisha Sonawane³

^{1,2}Student, Department of Computer Engineering, Shivajirao S. Jondhale College of Engineering, Mumbai, India

³Assistant Professor, Dept. of Computer Engineering, Shivajirao S. Jondhale College of Engg., Mumbai, India

Abstract: The cloud based applications authenticate users before they are allowed to access the services provided by them. Most of the commonly used user authentication mechanism is text-based password systems. Graphical passwords have been proposed because the picture format effect suggests that people have better memory for images. After a comprehensive study on various graphical password schemes, it is found that they suffer from vulnerabilities of shoulder surfing attack and teasing the user by using several steps during login. The important things of this research is to implement and provide a secure shoulder-surfing resistant authentication method by providing the variable size grid to select images during login phase. For resistance, two ways of inputting the password is possible with this method. In order to find security system, a shoulder surfing attacking session was conducted in the university with questionnaire utilized the user’s feedback on security of proposed method.

Keywords: Graphical password, authentication, shoulder-surfing, usability, security.

1. Introduction

Text based passwords are the most widely used for authentication. The shoulder surfing attack that can be performed by an antagonist to obtain user’s password by watching over the user’s shoulder as he enters his password. Traditionally, shoulder surfing attacks also called “peeping attacks” concerns moved from telephone calling card fraud to automated teller machine (ATM) fraud, and more recently to mobile computer users. In a psychological studies show that images are recognized with very high accuracy (up to 98 per cent) after a two-hour delay, which is much higher that accuracy for words and sentences. TEXTUAL based passwords have been the most widely used authentication method for decades.

2. Problem Definition

- **Problem Statement:** Text based passwords are the most widely used for authentication. But in this technique has its own flaws and is vulnerable to attacks.
- **Proposed Systems:** In this section we will consider a shoulder surfing resistant graphical password scheme based on Pass face Scheme . The Pass face scheme given by Real User Corporation is a recognition-based graphical password authentication scheme. This

method is enhanced in the proposed scheme to provide more usability and security.

Table 1
Literature survey

Sr. No	Author	Name	Year of Publishing	Description
1.	Syukri A, Okamoto E, Mambo M.	Springer Berlin/Heidelberg.	1998	A user searching system using signature written with mouse. Information Security and Privacy
2.	Chiasson S, van Oorschot PC,	Biddle R. Graphical password authentication using cued click points.	2007	In ESORICS 2007 Sep 24
3.	Wiedenbeck S, Waters J, Birget JC	Design and longitudinal evaluation of a graphical password system.	2005	International journal of human-computer studies
4.	Rao K.G., Vijayakumari R, Rao BB	4-Stage Graphical Password Authentication Scheme for Cloud	2017	Journal of Theoretical and Applied Information Technology

A. Existing Systems

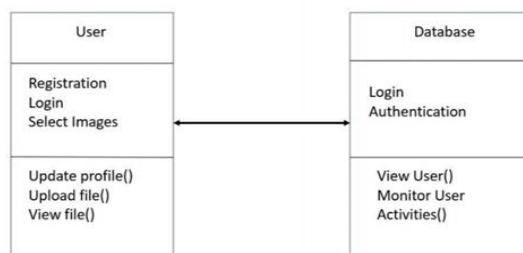


Fig. 1. Class Diagram of the process

Like other authentication methods, the graphical password consisted of two steps, registration and authentication. In the registration step, users select some images from different categories or produce a graphical image as his password. Later

on, in the authentication step, he needs to select the correct images or re-draw the graphical password which is used by him in the registration step. In the following, these two steps are explained in detail.

B. Registration

Since registration is the first step, each user needs to input his Username and password. If you are not register then you can register yourself by clicking on register here link. In a registration phase user have to enter his username first. Then he has to write a password of it then he has to re-Enter of that password also user has to enter his full name, college name, Email Address and phone number. The all fields are compulsory. Then user have to click on signup.

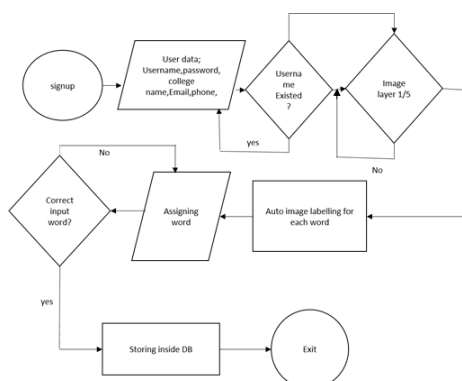


Fig. 2. Registration Flowchart

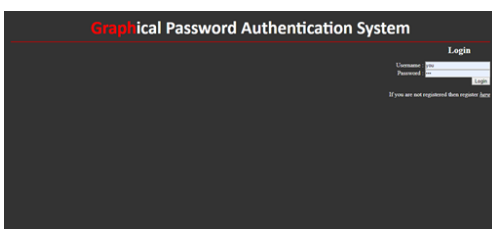


Fig. 3. Entering username and password for login

C. Authentication

In an Authentication process the there are five images containing words user have to remember of that word. there are 5 phases user has to select one word at each phase after passing of each phase user will get message user is successfully registered and user have to click here for login. Then user has to select the images where when he login himself in registration phase.



Fig. 4. User credentials as its username, name, Email and phone no.

In figure 4, user can change the sequence of images when he selects as password. And user also can change the password of his account in their user has to enter his old password and enter new password for updating of password. In this system user can upload his profile picture (.jpg,.jpeg,.gif,.png, JPG,.PNG,.GIF format). after click on upload user can see his uploaded profile picture.

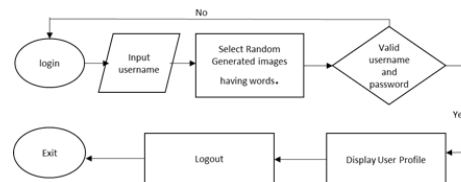


Fig. 5. Authentication flowchart

In the above figure the Authentication flowchart is shown.

D. Requirement Analysis

This phase started at the beginning of our project, we had formed groups and modularized the project. main points of consideration were:

Hardware Requirement:

- PC with 4GB RAM
- 250 GB HDD
- I3 and above
- 2.3GHz processor

Software Requirements:

- Technology Used: Java
- Database: MySQL
- Development Tool: PHP

3. Conclusion

This paper presented implementation of shoulder-surfing resistant graphical password system.

Acknowledgement

We sincerely wish to thank the project guide Prof. Manisha Sonawane for her ever encouraging and inspiring guidance helped us to make our project a success. Our project guide makes us endure with her expert guidance, kind advice and timely motivation which helped us to determine our project.

We also express our deepest thanks to our HoD Prof. P. R. Rodge & Deputy HoD Prof. Uttara Gogate whose benevolence helped us in making the computer facilities available to us for our project in our laboratory and making it a true success. Without their kind and keen cooperation our project would have been stifled to a standstill.

Finally, we would like to thank our college principal Dr. J. W. Bakal for providing lab facilities and permitting us to go on with our project and guide for project development. We would also like to thank our colleagues who helped us during our project.

References

- [1] Syukri A, Okamoto E, Mambo M. A user searching system using signature written with mouse. In *Information Security and Privacy*, pp. 403-414, Springer Berlin/Heidelberg, 1998.
- [2] Chiasson S, van Oorschot PC, Biddle R. "Graphical password authentication using cued click points," in *ESORICS*, Vol. 7, pp. 359-374, September 2007.
- [3] Wiedenbeck S, Waters J, Birget JC, Brodskiy A, Memon N. "Pass Points: Design and long term evaluation of graphical password system," *International journal of human-computer studies*, vol. 63, no. 1, pp. 102-127, July 2005.
- [4] Rao K.G., Vijayakumari R, Rao B. B. "4-Stage Graphical Password Authentication Scheme for Cloud," in *Journal of Theoretical and Applied Information Technology*, vol. 95, no. 1, pp. 105-114, January 2017.