Authentication Schemes For Session Passwords Using Text And Colors

[1]Nirmala.B, [2]Manigandan.T, [3]Kumanan.K
[1,2]M.E Student, [3]Assistant Professor
Department of Computer Science and Engineering
Sri Venkateswara College of Engineering

Abstract: Textual passwords are the most common method for authentication. But textual passwords are vulnerable to eves dropping, shoulder surfing. Graphical passwords are used as alternative technique to shoulder surfing. To address this problem, text can be combined with images or colours to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated. Two techniques are proposed to generate session passwords using text and colours which are resistant to shoulder surfing.

Keywords: Shoulder surfing- Graphical password- Session password

1. INTRODUCTION

The main aim of the project is to prevent shoulder surfing which is a technique of stealing information from users by watching over their shoulders. We use text based session password scheme which is capable of preventing shoulder surfing. The proposed system consists of two methods that the user undergo while entering the passwords. The first method is the pair based authentication scheme and the second method is the hybrid textual authentication scheme. According to these graphical password schemes, the user is allowed to access his account.

1.1. Shoulder surfing

Shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. It is commonly used to obtain passwords, PINs, security codes and similar data. Shoulder surfing is particularly effective in crowded places because it is relatively easy to observe someone as they fill out a form, enter their pin at an ATM, enter a password at cybercafé and in other public places. Shoulder surfing can also be done at a distance using binoculars or other vision-enhancing devices.

1.2. Graphical Password

Access to computer systems is most often based on the use of alphanumeric passwords. However, users have difficulty in remembering a password that is long and random-appearing. Instead they create short, simple, and insecure passwords. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and, therefore, more secure. Most often graphical passwords deal with images. Our graphical password scheme is text based and is aimed at making it easier to be used by people. Most of the graphical password schemes were introduced in order to overcome the disadvantages in text based passwords. But, unfortunately, not many of them turned out to be successful.

2. LITERATURE SURVEY

PBKDF2 Pair & Hybrid technique used in grid for session password generation. Hybrid textual scheme, ratings should be given to colors, based on these ratings and the grid displayed during login, session passwords are generated.

The session passwords provide higher security against various attacks such as dictionary attack, brute force attacks as password changes for every session.

Two authentication techniques based on text and colors are proposed for PDAs. These techniques generate session passwords and are resistant to dictionary attack, brute force attack and shoulder-surfing. Both the techniques use grid for session passwords generation. Pair based technique requires no special type of registration; during login time based on the grid displayed a session password is generated. For hybrid textual scheme, ratings should be given to colors, based on these ratings and the grid displayed during login, session passwords are generated.

3. PROPOSED SYSTEM

Figure 1 show proposed system architecture, the first method we are implementing a textual based authentication scheme in which we generate a grid interface containing alphabets and numbers. The user has to provide the username and password in the textual manner and that will be saved in the server for verification process. While login into the account, the user first enters their user id, then they have to enter the session password generated from the grid.

We also implement a Hybrid based authentication scheme in which a color interface is displayed. The user has to provide rating of the color at registration phase. Depending on this rating given, session password is generated. These schemes will be verified and then only the user is allowed to access the account.

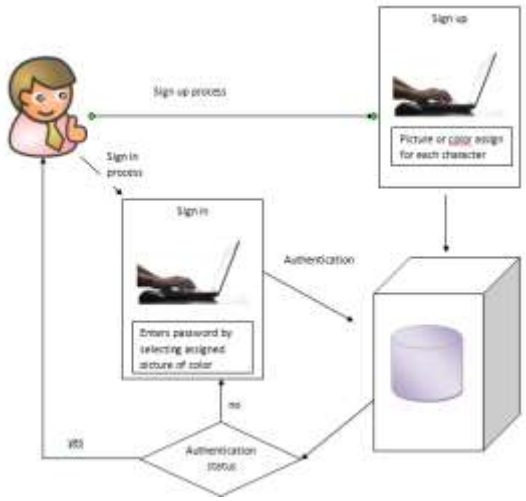

Figure 1 System Architecture

3.1. User Interface Design

In this module we are going to create an user application by which the user is allowed to access the data from the server. Here first the user needs to create an account and then only they are allowed to access network. Once the user creates an account, they are allowed to login into their account to access application. Based on the user's request, the server will respond to the user. All the user details will be stored in the database of the server. In this project we will design the user interface frame to communicate with the server through network coding using the programming languages like Java/ .Net.

3.2. Monitoring Server

The server will monitor the entire user information in their database and verify them if required. Also the server will store entire user information in their database. Also, the server has to establish the connection to communicate with the users. The server will update each user's activities in its database. The server will authenticate each user before they access the application. The server will thereby help in preventing the unauthorized user from accessing the application.

3.3. Pair-Based Authentication Design

During registration user submits his password. Maximum length of the password is 8 and it can be called as secret pass. The secret pass should contain even number of characters. Session passwords are generated based on this secret pass. During the login phase, when the user enters his username an interface consisting of a grid is displayed. The grid is of size 6 x 6 and it consists of alphabets and numbers. These are randomly placed on the grid and the interface changes every time. User has to enter the password depending upon the secret pass. User has to consider his secret pass in terms of pairs. The session password consists of alphabets and digits. The first letter in the pair is used to select the row and the second letter is used to select the column. The intersection letter is part of the session password. This is repeated for all pairs of secret pass.

3.4. Hybrid Textual Authentication Design

The User should rate colors from 1 to 8 and he can remember it as "RLYOBGIP". Same rating can be given to different colors. During the login phase, when the user enters his username an interface is displayed based on the colors selected by the user. The login interface consists of grid of size 8×8. This grid contains digits 1-8 placed randomly in grid cells. The interface also contains strips of colors. The color grid consists of 4 pairs of colors. Depending on the ratings given to colors, we get the session password.

3.5. Authentication And Application Access

In this module the server will verify the password provided by the user and verify them with the database values and then only the users are allowed to access the application. If the user enters the incorrect password then the server will not allow the user to enter and access the application. So that we can prevent the application from unauthorized user access.

4. RESULTS

Figure 2 Online Purchase Website

Figure 3 Authentication to generate Session Password

Figure 4 Entering Session Password using Colors

Figure 5 Session Password Verification

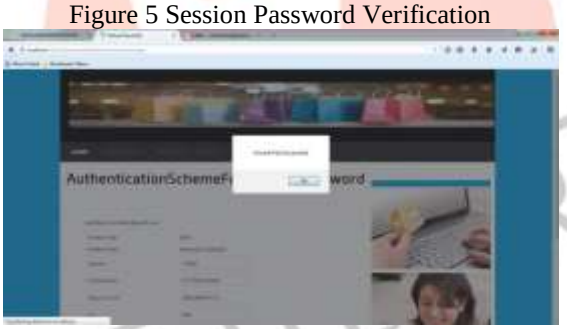

Figure 6 Payment Success

5. CONCLUSION AND FUTURE WORK

In this authentication schemes since the password is used only during registration it is hard to guess the password through shoulder surfing, eves dropping. The first scheme is as usual as the normal registration method and during login the user has to select the password from the grid displayed. In the second scheme user has to rate the colors and in login the user must enter the password based on the grid displayed and is verified. Only session passwords are used during login and transaction. This shows that the proposed authentication scheme is resistant to shoulder surfing. However these schemes are completely new to the users and the proposed authentication techniques should be verified for usability and effectiveness.

In future pair based and Hybrid textual authentication schemes are not used in any online shopping applications. So the shopping sites can adopt this authentication scheme for improving their security. Besides, this scheme can be used in any other application where the security is the main concern.

REFERENCE

[1] Z.Zheng, X.Liu, L.Yin, Z.Liu "A hybrid password authentication scheme based on color and text" Journal of computers-May 2010.

[2] S.Balaji, Lakshmi.A, V.Revanth, M.Saragini, V.Venkateswara Reddy "Authentication Techniques For Engendering Session Passwords With Colors And Text" Advances in Information Technology and Management Vol. 1, No. 2, 2012.

[3] Rohit Jagtap, Vaibhav Ahirrao, Vinayak Kadam, Nilesh Aher, "Authentication schemes for session password using color and special characters" International Journal of Innovations & Advancement in Computer Science, April 2014.

[4] M.Sreelatha, M.Shashi, M.Anirudh, MD Sultan Ahamer, V Manoj Kumar,"Authentication schemes for session passwords using color and images", International Journal of Network Security & its Applications(IJNSA), May 2011.