A ROBUST TECHNIQUE FOR PASSWORD SECURITY

Sandhya Samant[1], Jaspreet Srivastava[2], Abhishek Mittal[3]
[1,2,3]Quantum Global Campus, Roorkee

Abstract

In the present digital world, computer security and authentication has become an important issue for computer users to protect their data from the impostors and intruder's.Security of data completely depends on the password. A password is a secret word or phrase (combination of alphabet, numbers, and special character) that allows the user to access the system resources. Here we are providing an authentication scheme which is a solution to this problem by making a spy-resistant password entry module that looks as a Keyboard or virtual keyboard to improve more security on publicly observable environment .This authentication technique gives a secure login interface which uses randomly Generated Single Integer Input Digits corresponding to password characters on secure login interface module.

Keywords: random number generation, authentication scheme, secure login interface etc.

Introduction:

To provide security we use traditional password authentication schemes but that too have many drawbacks. In password mechanism the password length are usually small or short, thus making it easier to spy and memorize the passwords via monitoring of keystrokes or through eavesdropping [1, 2].

In our solution we are trying to make a spy-resistant password entry module that looks like Keyboard or virtual keyboard to improve more security on publicly observable [3, 4]. In this approach a security method is proposed to provide a strong security support anywhere for both short and long character-password at user level. We are developing a user authentication technique by providing a login interface. The password will consist of text and the image for verification at every login .This approach does not require the input code to be hidden from anyone or converted to placeholder characters for security reason. The system accepts all printable ASCII characters, which may consist of lower and upper case (A-Z, a-z), numeric digits (0-9), and special characters (@ * $ + ~ - ! _ ^, ( ) { } # % etc).

In this, A login user interface is designed that has all alphabets (upper and lower case letter), numeric digits and special characters and an image, at the time of entering numeric digits as a password instead of character that is corresponding of each letter and is called Randomly Generated Single Integer Input Value (0-9) on login interface and every time user login then he will get new integer input value corresponding to the characters to produce a hardened password that is convincingly more secure than conventional password entry system against both online and offline attackers. It means a single integer input value is assign more than one letter (A-Z, 0-9, a-z, (@ * $ + ~ - ! etc.) makes it impossible for attackers to hack or electronically eavesdrop, shoulder surfing, brute force attack on user password at input level (at application layer). It will improve the security and integrity of the password systems. Whenever an intruder tries to spy he will get only numeric digits that are assigned more than one letter.

Structure of the System

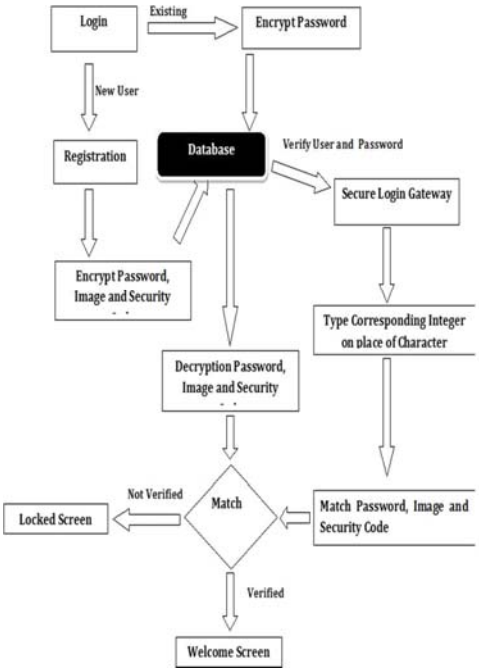

Figure 1 DFD of Proposed System

The architecture of the approach is shown in fig.1. In this we can take maximum 6 characters length password that must contain one Upper & lower case alphabet and one integer number and maximum length of password depends on coder and maximum password length provide more security.

Working:

Step 1.Splash Screen

This is the first screen (Fig 2), the user gets when it first interacts with the system

Figure 2 Splash Screen

Step 2.User Phase

Login Module. In this module the user gets the input screen (Fig 3).

Figure 3 Login Module

If the user is registered user then it enters its credentials which are customer id and password.

Firstly it will create the connection with the server. When connection will be verified it will send the customer id to the server and retrieve the encrypted password. After this we decrypt the password and compare with the password entered by the user. If password matches it will move to secure login gateway otherwise display the failure message.

Registration Module:
If the user is the new user then he/she clicks on the register now button , which will make the user jump to registration form(Fig 4)where the user registers its name, user id , password, account number ,image and a secret code. Then finally clicks on register now button.

Figure 4 Registration Form

The password, secret code and the image code will be stored in database in encrypted form. The database (DB) contains all the credentials of legitimate users. We have restricted the password length maximum up to 6 characters and secret code of 3 characters which are alphanumeric.

Step 3.Secure Login Interface

After creating our password followed with a Strong password points ,now User goes to Secure login interface Form in which lower and upper case letter (A-Z, a-z), numeric digits (0-9), and special characters (@ * $ +- ! _ ^, ( ) { } # % etc) available with a corresponding randomly Generated single Integer value (0-9) and this integer value is changed every time when user login (Fig5). At this time the user enters the corresponding integer values with respect to password and secret code. At the time also the user selects the image from the five available one corresponding to its original selection while doing the registration

Figure 5 Splash Screen

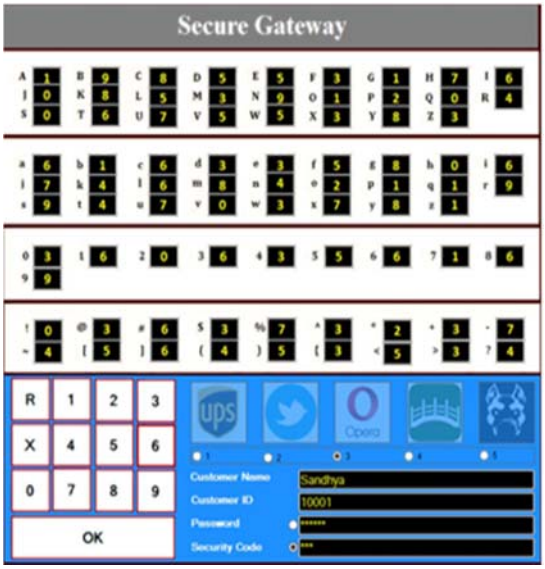

Figure 6 Secure Login

At this step user enter own password in the form of numeric value instead character that is correspond to valid password characters after studying the secure login user interface It may the number correspond to a letter is repeated. And our algorithms make a table of every unique single integer that is entered by user (in the form of Jagged array as a backend process).

Step 4. Access Given

If the credentials entered by the user are correct in STEP 3 then user is given access to account and thus welcome screen is flashed.

Step 5. Access Denied/Account Blocked

If the credentials entered by the user are incorrect in STEP 3 then user is given message as wrong input .The maximum trial for inputting credentials is three. After this account will be blocked and account blocked screen will be flashed.

Conclusion:

In this approach Randomly Generated Single Integer Input digits corresponding to password characters on login interface module. This makes it impossible for attackers to hack or electronically eavesdrop, shoulder surf, or use brute force attack on user password at input level (at application layer). It will improve the security and integrity of the password systems. We believe that a scheme that is simpler for the user, more efficient or less time consuming in terms of login time and more secure against the aforementioned attacks can be developed.

References:

1. Kessler, Gary C., 2002. “Passwords - Strengths and Weaknesses”. Jan 1996.URL:http://www.garykessler.net/library/password.html.
2. I. Scott MacKenzie, “KSPC as a Characteristic of Text Entry Techniques”,Dept. of Computer Science, New York University
Toronto, Ontario, Canada M3J 1P3.
3. Desney S. Tan, Pedram Keyani & Mary Czerwinski. “Spy-Resistant Keyboard: Towards More Secure Password Entry on Publicly Observable Touch Screens”.
4. Mark S., (2005), “Information Security, Principles and Practice”, Wiley Interscience.
5. http://en.wikipedia.org/wiki/Passive_attack .
6. Kessler, Gary C., "Two-Factor Authentication for Online Banking Applications". Department of Applied Aviation Sciences - Daytona Beach. Paper 14. http://commons.erau.edu/db-applied-aviation/14
7. The Author Engin Kirda, Christopher Kruegel -- Technical University of Vienna 2005. Published by Oxford University Press on behalf of The British Computer Society. “Protecting Users Against Phishing Attacks”.
8. X. Suo, Y. Zhu, G. S. Owen, "Graphical Passwords: A Survey, " 21st Annual Computer Security Applications Conference (ACSAC'05), pp. 463-472, 2005.
9. Fujita, K. and Y. Hirakawa, 2008, “A study of password authentication method against observing attacks”, 6th International

Symposium on Intelligent Systems and Informatics, SISY 2008.
10. Sarvar Pate1, “Number Theoretic Attacks On Secure Password Schemes”, 1997. IEEE.
11. Mohammad Shahid, Mohammed A Qadeer. 2009. “Novel Scheme for Securing Password”, 2009. 3rd IEEE DEST '09, Digital Ecosystems and Technologies Digital Ecosystems and Technologies Conference.
12. Hea Suk Jo, Hee Yong Youn. “A Secure User Authentication Protocol Based on One-Time-Password for Home Network”, International Conference, Singapore, Springer, May 2005, pp: 519-528.
13. S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon," Authentication using graphical passwords: Basic results", Human Computer Interaction International (HCII 2005), Las Vegas, July 25-27, 2005.
14. Xuguang Ren, Xin-Wen Wu, “A Novel Dynamic User Authentication Scheme” International Symposium on Communications and Information Technologies (ISCIT), 978-1-4673-1157-1/12, 2012 IEEE
15. Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and Waqas Haider, “A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication”, World Applied Sciences Journal 19 (4): 439-444, 2012 ISSN 1818-4952; © IDOSI Publications, 2012.
16. Anand Sharma and Vibha Ojha et al.,” Password Based Authentication: Philosophical Survey”, 2010 IEEE.