International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 2 278 - 279

Web Login Security & Authentication using Dynamic Password

Mr. R. B. Nimbalkar
Department of E&TC
P. Dr. V. V. Patil
Inst. of Engg. & Tech. Loni
rbn_nimbalkar@rediffmail.com

Mr. S. B .Lavhate
Department of E&TC
P. Dr. V. V. Patil
Inst. of Engg. & Tech. Loni
lavhate_sb@yahoo.com

Mr. N. D. Toradmal
Department of E&C
Government Polytechnic,
Malvan
nitintoradmal.vlsi@gmail.com

Abstract- In day to day life we use the password to access the e-mails, accounts on the different websites, social media websites & apps etc. The passwords used are generally text password having any combinations of letters, numbers & special characters & that passwords are static. Many times the users not changes their Passwords are vulnerable to interception. Here we proposed a method to change the password automatically. So the passwords are not static & the part of password will change every time you will enter the password i.e. every time user password is different from its previous.

Keyword- *Dynamic Password, Server, Security.*

*****

I. Introduction

A password is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource, which should be kept secret from those not allowed access. The easier a password is for the owner to remember generally means it will be easier for an attacker to guess.

The security of a password-protected system depends on several factors. The overall system must, of course, be designed for sound security, with protection against computer viruses, man-in-the-middle attacks and the like. Passwords should be chosen so that they are hard for an attacker to guess and hard for an attacker to discover using any (and all) of the available automatic attack schemes. The rate at which an attacker can submit guessed passwords to the system is a key factor in determining system security. Some systems impose a time-out of several seconds after a small number (e.g., three) of failed password entry attempts. In the absence of other vulnerabilities, such systems can be effectively secure with relatively simple passwords, if they have been well chosen and are not easily guessed. The chances of offline guessing attacks are also more & many time these password are guessed by the attackers. Most of the password generators generates the password which is difficult to remember & based on their program logic. Here the password logic is defined by user & hence easy to remember. [1][2][3]

II. Related Work

The password we are using for login for our personal computer, mobile phones &also while accessing the e-mails, social media websites & other internet services most of the time passwords are static. We change the password rarely & hence mostly such passwords may be guessed by attackers. So to solve these problems we may change our password every time we login. It can be done by some server side modifications. Password managers differ in many aspects, including database format, functionality and availability of source code, supported platforms and access to cloud storage. Some popular password managers invent their own database format, used exclusively by them. This is especially true for the password managers embedded in major browsers. [4] [5]

The password entered by user is compared with the server database. The main storage methods for passwords are plain text, hashed, hashed and salted, and reversibly encrypted, but the password remains static which is defined by user. Here in this paper a new format is suggested to store the password in which- The password must be greater than eight characters The first four character remain same & the control character (it may changed by user after login in change control field activity) is a mathematical or polynomial or logical field which decides the relation between the next characters or digits.

When user enters the password depending upon the control character / digit he has to enter the next characters. The operation decided by control field which is defined by user itself according to that server will take action. The control character & sequence of operation to find the relation between the fields is decided by user. Mathematical, polynomial or logical operation & its sequence is decided by user in password management activity. During the first login the server will ask for login name & after that it will ask for password. Before confirming the password server will ask some questions like enter the control field after entering the control field it will ask for mathematical, polynomial or logical expression to identify the relation between the changing field, after selecting the expression server will ask to enter the remaining fields. The Password format is as shown below

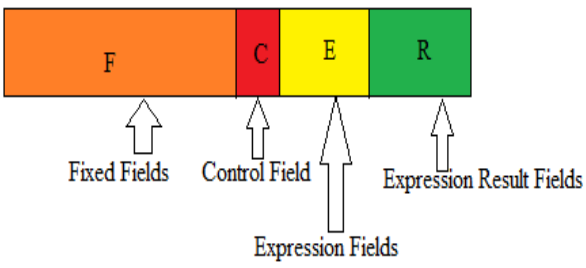

Fig. 1. Password Format

1. Fixed Fields (F):-
This is variable length field depending on user. The entries in this field may be letters, special characters or may be digits. It is not necessary to change these fields.
2. Control Field(C) :-
This is a control field & which selects the expression defined by user.
The Expression may be arithmetic, polynomial or logical.
3. Expression Field (E):-
In this field the user enters the values required to execute the expression decided by control field. Every time when user enters the password for login these fields will change hence previous entered values for expression are not allowed again, hence user has to enter new values to execute expression.
4. Expression Result Field (R):-
This field gives the result of expression. When user enters the password, he / she enters the last characters as a result of expression selected by he/ she in control field. Then the result of expression is compared with the result stored in server database & if both the result matches then the access is given to the user otherwise access is denied by displaying the message username or password is wrong. For example the password is abcd@123459 In this password fixed fields are abcd@12, 3 is control field which defines the mathematical operation addition of next fields i.e. 4 & 5 and last field is expression result which is 9. The expression field values are allowed to enter one time only. When user enters the same values the server will deny the access by displaying the message username or password is wrong.

III. Flow Chart:

Flow chart for Server & Client (User) is as shown below

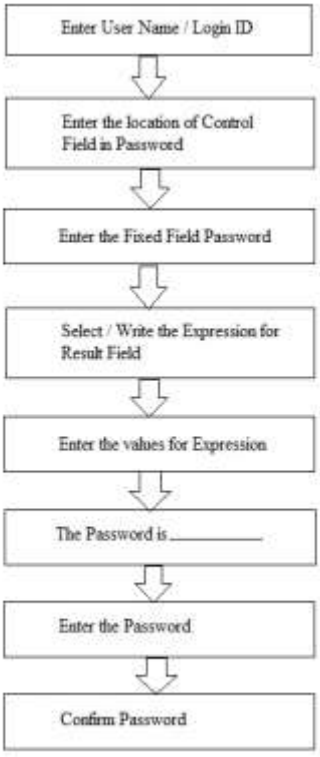

Fig. 2 Flow Chart 1(User)

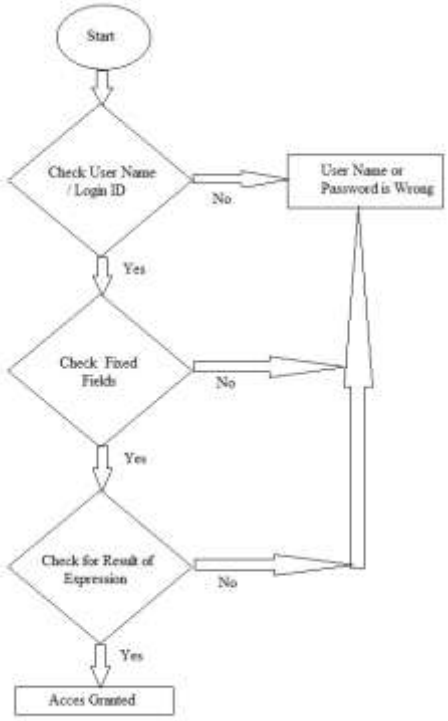

Fig. 2 Flow Chart 2 (Server)

IV. Application:-

This technique can be used in web browser application & other application where biometric & other authentication technique cannot be used. It is also used for personal locker application.

V. Conclusion:-

In this technique the password will change every time when entered by user & hence it is difficult for attackers to guess the password. It does not require any additional hardware.

Acknowledgement

We would like to take this opportunity to express our gratitude towards our chairman, Padmabhushan Shri Balasaheb Vikhe Patil (Ex. Minister, Heavy Industries, Government of India),), our trustee Hon'ble Dr. Ashok Vikhe Patil CEO, Pravara Rural Education Society, Loni, Tal-. Rahata, Dist. - Ahmednagar, (Maharashtra), Prof. N. G. Nikam P. Dr. Vitthalrao Vikhe Patil Polytechnic, Loni for their guidance, advise and providing facilities for our research.

References

[1] Paolo Gasti and Kasper B. Rasmussen "On The Security of Password Manager Database Formats."
[2] Jianxin Yan, Alan Blackwell, Ross Anderson, Alasdair Grant "The Memorability and Security of Passwords Some Empirical Results"
[3] https://en.wikipedia.org/wiki/Password
[4] Jonathan Katz, Rafail Ostrovskyy, Moti Yungz "Efficient and Secure Authenticated Key Exchange Using Weak Passwords"
[5] Blake Ross, Collin Jackson, Nick Miyake, Dan Boneh, John C Mitchell "Stronger Password Authentication Using Browser Extensions"