Secured Password Authentication Scheme

Sandhya Samant[1]
Lecturer,
Quantum School of Technology, Roorkee

Deepak Painuli[2]
[2] Assistant Professor, Department of CSE,
Quantum Global Campus, Roorkee

Ashish Gupta[3]
[3] Assistant Professor, Department of CSE,
DBIT, Dehradun

Abstract:

In the present era computer security and authentication has become an important issue for computer users to protect their important data from the impostors and intruders. Many access applications depend on the general password authentication. A password is a secret word or phrase (combination of alphabet, numbers, and special character) that allows the user to access the system resources. The password assists in ensuring that unauthorized user don't access the resources. A single local computer network may have hundreds or thousands of password-protected accounts and only one need to be compromised to give a attacker an entry to the local system or network. Usually the password length is small or short, thus making it easier to spy and memorize the passwords via monitoring of keystrokes or through eavesdropping. Here we are providing 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 login interface module.

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

Introduction:

To provide authentication we use traditional password authentication scheme but it still has a few important drawbacks. One of the major weaknesses is that the strength of the password depends mostly on the user and most commonly attack is performed in crowded places because it's easy to stand next to someone and watch as they enter a password or PIN number at an ATM machine, where the attack can be launched and not noticed.

A password is usually a secret string of character used to authenticate an entity or gain access to a resource or services. User names and passwords are commonly used by people in the login process time that controls access to protected systems and services. The name pass-code is used when the password consists only of numeric digits such as personal identification number (PIN).The main problem with password is that they may be forgotten, stolen, spoofed, eavesdropped, shoulder-surfed or guessed by an intruder [3].

In this approach an authentication method is proposed to provide a strong security support anywhere for both short and long character-password at input 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, 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.

Related work:

Kazuhide Fujita, Yutaka Hirakawa[6] proposed the authentication method which was secured against the observing attacks. The proposed method resists against the Brute force and also resists attack using a video recorder (video recording attack). It does not require any special hardware. In this the video recording attacks are considered that attackers analyze videos to obtain other person's password, where user's password entry task is recorded once or two times .

Mohammad Shahid, Mohammed A Qadeer[8] presented five novel schemes as 1. Moving Balls based Security Scheme,2. Picture Based Password Security Scheme,3. Encrypted key Based Security Scheme, 4. Expression Based Security Scheme, and lastly 5. Varying Based Password Security to protect passwords and will prove robust against common security attacks like dictionary attack, brute force attack, shoulder surfing attack problem, forgery and social engineering .

Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and Waqas Haider[10] described various password attacks such as dictionary attacks, brute force attacks, video recording attacks, shoulder surfing, replay Attacks, phishing, key Loggers etc and comparative analysis of different authentication methods such as conventional password scheme, virtual passwords, graphical passwords, biometrics, key stroke dynamics, click patterns etc. User must know the password attack and then should apply suitable authentication method according to situation because some of the methods are applicable at stand alone system and some are applicable at online environments as over ATM and some internet services .

Anand Sharma and Vibha Ojha et al[11]. presented study of attacks on password based authentication and their prevention points. They divided these attacks in three main categories such as Attacks on the system end (password guessing), Attacks on the communication channel (replay and man-in-the-middle attacks), Attacks on the user end (social engineering, shoulder surfing and phishing).

Sarvar Patel[7] proposed a password-based protocol. it promises security not only against active attacks but also against offline dictionary attacks, is known as Encrypted Key Exchange (EKE) that allows two parties sharing a password to exchange legitimate information over an insecure network by using a grouping of public and secret key cryptography. . He has exposed how an attacker is capable to find out the secret passwords in the RSA variants of Direct Authentication and Secret Public Key protocols and explored why such attacks are successful against apparently secure password protocols and also shown attacks against half encrypted versions of Encrypted Key Exchange .

Xuguang Ren, Xin-Wen Wu[9] proposed a secure dynamic user authentication scheme, Unlike the traditional password authentication or two-factor authentication their authentication scheme treat OTP as a category of dynamic one-time password (OTP) against the replay attack or man-in-the-middle attack and this OTP is valid for only one login session which can be change with the time. OTP generation is used to achieve spacing dynamism. To achieve timing dynamism property of the OTP, the time factor is included into the generation procedure. Current methods have been used to generate OTP are Time synchronized or Mathematical algorithms. In Time-synchronized method the OTP change with the time and never repeats but in Mathematical algorithms based on the previous password or also generate non-repeat OTP each time .

Dawei Hong, Shushhuang Man, Barbra Hawes et al[10]. proposed a new password scheme which is strongly resistant to spyware and analyze the security of this scheme. in this at each time of login, system challenges(an icon or image or symbol on the login screen) to a user who wants to login. A login screen is divided into grids and each grid contains an icon or image or symbol and user also enter password that is a set of random strings, when a new user create a password he choose all 121 icons from an icon library on the server, he also determines 4 pass-icon and each icon has 4 variation and the user determines the string correspond to a variation and entered the strings beneath the variation. It seems like a combination a graphical password and textual password scheme .

Proposed Architecture:

In fig 1, we have shown our proposed Secured Password Authentication Module Architecture.

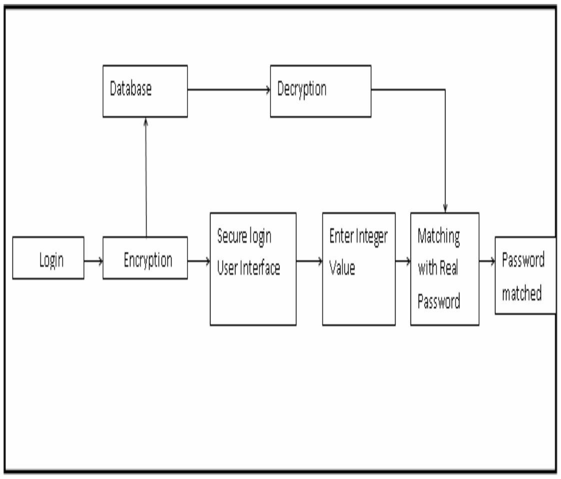

Fig.1 Secured Password Authentication Module Architecture

The figure is explained with the help of following steps.

Step 1.

First the user registers itself by giving name, id and password which is the combination of text and image.all these details are stored in a database ,where password is stored in a encrypted form using AES.

Step 2.

After creating the password, the user login through the secure login interface which contains 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.

Step 3.

The login interface is refreshed after every few seconds, this the user can do manually or can be refreshed automatically at each login.

Step 4.

In this step , the user enter own password in the form of numeric value instead of character after studying the secure login user interface. It will be the number corresponding to a letter, 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). At this step the user will also select the image from the displayed ones which will correspond to the original image.

Step 5.

At this step matching will be done between the entries obtained from login interface and the data saved in database. if this match is true then user gets the message as password matched and thus this provides the secure login to the user.

Conclusion:

In this scheme the security is provided with the help of Randomly Generated Single Integer Input digits corresponding to password characters and image selection on login interface module 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. 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, as, in our own experience.

References:

1. Kessler, Gary C., 2002. “Passwords - Strengths and Weaknesses”. Jan-1996. I.Scott MacKenzie, “KSPC as a Characteristic of Text Entry Techniques”, Dept. of Computer Science, New York University Toronto, Ontario, Canada M3J 1P3.
2. **Error! Hyperlink reference not valid., Error! Hyperlink reference not valid..** “A Secure User Authentication Protocol Based on One-Time-Password for Home Network”, International Conference, Singapore, Springer, May 2005, pp: 519-528.
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. 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.
6. Sarvar Pate1, “Number Theoretic Attacks On Secure Password Schemes”, 1997. IEEE.
7. 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.

8. 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

9. 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.

10. Dawei Hong, Shushhuang Man, Barbra Hawes, Manton Matthews, "A Password Scheme Strongly Resistent to Spyware".

11. Anand Sharma and Vibha Ojha et al.," Password Based Authentication: Philosophical Survey", 2010 IEEE.