MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 – 6953

Reshma Dilip Kadam
Computer
KJCOEMR
Pune,Maharashtra

Swapnil Dilip Koshti
Computer
KJCOEMR
Pune,Maharashtra

Amol Rajendra Gawde
Computer
KJCOEMR
Pune,Maharashtra

Prashant Chandrakant Kamble
Computer
KJCOEMR
Pune,Maharashtra

Prof. Bogiri Nagaraju
Computer
KJCOEMR
Pune,Maharashtra

Authentication Schemes for Session Passwords using Hybrid and Paired based Techniques

Abstract

Early we use Textual passwords as a security but these passwords are vulnerable to the various attacks like Dictionary attack, Shoulder surfing, eves dropping, etc. Further graphical passwords are coming to the existence but the graphical passwords have their own disadvantages like they require more time to Authenticate and the usability issues.
Thus we proposed a session password scheme in which the passwords are used only once for each and when session is terminated the password is no longer in use.
The proposed of session password scheme uses Text and colors for generating session password. Two session password schemes are used Hybrid Textual Authentication Scheme and Pair-based Authentication scheme.

Keyword : *Authentication, Password, Pair-based Authentication scheme*

1.INTRODUCTION

The common method which we used earlier is a Textual password in which the password which are lengthy is consider as secured password but the lengthy passwords is difficult to remember thus the user pick short password but short password are easily crack or hack. The new technique is proposed which is graphical password and biometric. This graphical password technique overcome the shoulder surfing problem in Textual password but these techniques have also some limitations and disadvantages like more time for Authentication and it's quite expensive.

So we proposed new password authentication technique is Session password .In which two new schemes are used Hybrid Textual Authentication Scheme and Pair-based Authentication scheme. Its gives the options for user to select the password as a color or alphanumerical grid.

When user logins into the system new session is created and that session is remains until user gets log out. For each new session new password is generated by system and that password is only valid for that particular session. When session is terminates the password is no longer

2. DESCRIPTION

Now a day's hundreds of millions of peoples using internet daily and day by day they are increasing. Today for authentication user name and password is used the basically .so the security must be provided in order to prevent hackers from accessing the account data. So authentication must be secure in order to protect user accounts. Authentication is provided by using two new techniques i.e. pair based authentication scheme, hybrid textual authentication scheme. The user has to select the authentication scheme at a time of login. In a pair based scheme Textual passwords are provided and in Hybrid Textual scheme set of colours is provided.

2.1Pair based scheme*:* At the time of registration user has to enter password. The minimum length of password is 8 characters. So at the time of login we create session password based on users original password entered at the registration time by using 6x6 matrix grid provided on login page.

Fig 1: The login interface

***2.2 Hybrid Textual scheme*:** At a time of registration user has to rate the colures from 1 to 8. So at the time of login set of colures is provided in random sequence. So user has to generate session password by using colures rating and grid provided on login page.

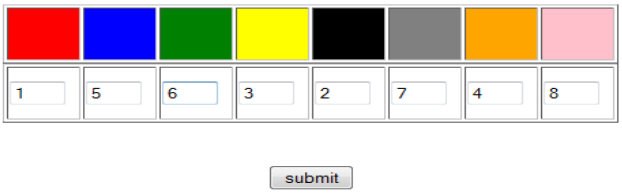

Fig 2: Rating Of Colours By User

The session password generated on login page is valid for that particular session only. Log is maintained at server side for session password generated at every session.

3. IMPLEMETATION

First time user does the registration on a particular website at that time user has to provide a password and rating of colours. This password and the colour rating is stored in database which is in a encrypted form. For these encryption SALT techniques is used. On the login page user can have two choices for selecting a password i.e. Hybrid Textual scheme and Pair based scheme. Then user can choose one of the schemes as per user comfort. After the choosing any one of scheme then login page is redirected to that technique.

If the user chooses the pair based scheme in this technique the user has to consider his/her password in terms of pairs. The pair based technique consist alphabets and digits. This alphabets and digits are in 8x8 matrixes. In this matrix no alphabets and digits are repeated and these alphabets and digits are in random manner and it will change each time when the new session is started or we refresh that page. The first letter in the pair is used to select the row and the second letter is used to select the column.User has to select intersection character as password for that particular session only.

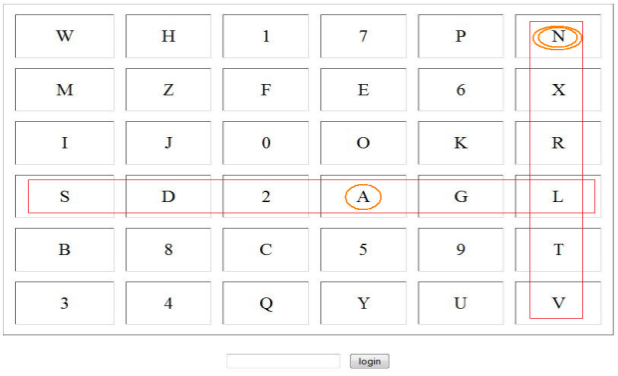

Fig 3: Intersection letter for pair AN

M12-1-2-7-2014

If the password length is n then session password length = n/2. When particular session is end then password for that session is also destroyed.

3.1Paired based scheme: 8x8 matrix is used to represent alphabets, digits and special symbols to the user so user has to select session password by using grid. *E.g.* Length of the password is 8 and password is ABCDEQRS. Now we will make pairs as AB CD EQ RS .so the session password length is 4. We will select row containing character A and column containing character B. And intersection of that row and column is inserted into the password field likewise all the pairs are selected into the grid and password is entered. This new password is valid only for that session and is stored in the user log on server. The session password and 8x8 grids is sent to the server. On the server side this session password is cross checked with the user's original password.

3.2 Hybrid textual scheme: Set of 8 colours is provided at the time of registration and user has to rate the colours from 1 to 8 when user selects hybrid textual as a Authentication scheme on login page user has provided the pairs of colours in random fashion. Then user has to select the colour pair. Rating of first colour is selected as row and rating of second colour is selected as a column intersection is entered into password filed. Likewise all the pairs are selected into the grid and password is entered.

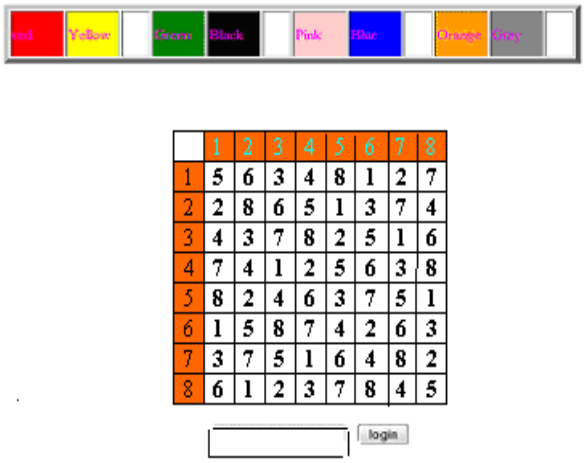

Fig 4: Login interface

This new password is valid only for that session and is stored in the user log on server. The session password and 8x8 grid is sent to the server. On the server side this session password is cross checked with the user's original password.

4. SALT *(*Cryptography*)*

In Cryptography, a salt is random data or string that is used as additional input to a function that hashes a password. The main function of salt is to protect against dictionary attacks and rainbow table attacks. A salt is randomly generated string for each password. The generated salt and User's password are concatenated and processed with the Cryptographic hash function and result is stored with salt in a Database. Hashing allows for late authentication

while defending against compromise of the plaintext. Cryptographic salts are used in many Computer systems like UNIX system and Internet security.

There are two types of salt first is fixed salt and second is Variable Salt. Fixed salt is a sequence of bytes which is used for concatenating with every password. We can keep this salt hidden and consider its providing security but it makes our system more vulnerable. The Variable salt is safer option as compare to the fixed salt because this is generated or computed separately for each password for concatenation with original password. It allows each stored password decoupled from the others and improving security against attacks.

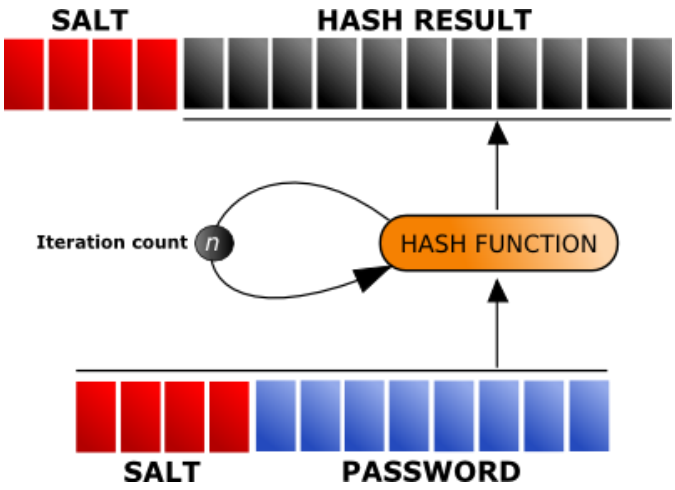

Fig 5: Generating Salt hash password

Steps for generating Salt Hash password:

1. Get password.
2. Generate Salt using random function.
3. Append salt to original password.
4. Generate Salt Hash password using appropriate hash function.
5. Finally store Salt and Salt Hash in the Database.

According to above steps Hash Password is generated. First original password is taken from the user and using Random function Salt is gets generated. After this generated Salt is appended to the original user's password. Then this Salt appended password is passes to Hash function. This Hash function is used to generate Salt Hash Password. Finally this generated Salt Hash Password and Salt is stored in database.

In this iteration count is used which is refers to the number of time that the hash function with which we are digesting is applied to its own this means that, once we generate a salt and

concatenated with the password then apply the hash function, get the result and again pass that result as a input to the same hash function .This process is repeated again and again a number of times. The minimum number of iteration is 1000 for more security.

5. PBKDF2 (Password Encryption)

Pseudorandom function such as cryptographic hash, cipher is applied by PBKDF2 to the user password along with salt value. This process repeated multiple times to produce derived key. This key is used as cryptographic key in subsequent operations. Having a salt added to the password reduces the ability to use recomputed hashes for attacks, and means that multiple passwords have to be tested individually, not all at once. The standard recommends a salt length of at least 64 bits.

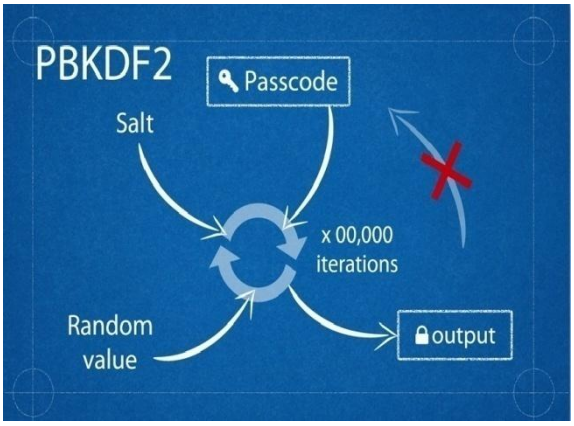

Fig 6: Password Encryption

PBKDF2 is used for generating derived key along with value of salt. So PBKDF2 algorithm takes an salt, Random function which gives random value , original user's password . Then this algortihm using number of iterations again and again Derived Key is generated which is final output. Derived key that conations salt, some random vlaues and original password. This is for the logn passkey which is makes craking or hacking of password is quite slow and makes paswword more secure and protected.

5.1 Key derivation process of PBKDF2 in this key derivation function has five parameters:

DK= PBKDF2(PRF, Password, Salt, c , dkLen)

Where:

- PRF is a pseudorandom function.

- Password is the master from which a derived key is generated.
- Salt is a generated cryptographic salt.
- c is the number of iteration in hash function.
- dkLen is the desired length of derived key.
- DK is the generated derived key,

6. TECHNOLOGIES USED IN THE SYSTEM

- *Pair based authenticate scheme*
- *Hybrid Textual scheme.*
- *PBKDF2-Password-Based Key Derivation Function 2*
- *AES-Advance encryption standard.*
- *salt*

7. CONCLUSION

The existing techniques does not have that much capability to secure password from hackers or third party location .because in this techniques only one password is used for each and every session and password is transfer for authentications of users. So these passwords are easily hacked by hackers. We proposed a system called Session password ,in this it provides a new password for each session and need not to transfer password form server each time for authentication purpose that's why Session password scheme provides more security than the other existed systems.

8. FUTURESCOPES

Future scope of this technique is that , as it provides more security than the others existed systems more secure login of users is possible .so this technique is not just limited for PDA i.e. personal digital Assistant but also it is very useful for providing protection against Hacking, Dictionary attacks ,etc. In future it will be used for Banking Applications, Mobile phones applications where the security is more important. It also use with the 3D password technique for providing more and more security.

ACKNOLEGEMENT

First and foremost, we would like to thank our guide Prof. Bogiri Nagaraju, for his guidance and support. We will forever .remain grateful for the constant support and guidance extended by guide, for completion of project report. Through our many discussions, he helped us to form and solidify ideas. The valuable discussions we had with him, the penetrating questions he has put and the constant motivation, has all led to the development of this project. We are

also thankful to our family members for their encouragement and support in this project work.

REFERANCES

[1]. R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.

[2]. Real User Corporation: Passfaceswww.passfaces.com

[3]. Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., "The design and analysis of graphical passwords" in Proceedings of USENIX Security Symposium, August 1999.

[4]. A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer- Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[5]. G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

[6]. HaichangGao, ZhongjieRen, Xiuling Chang, Xiyang Liu UweAickelin, "A New Graphical Password Scheme Resistant To Shoulder Surfing.

[7]. S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, "Design and longitudinal evaluation of a graphical password system". International J. of Human-Computer Studies 63 (2005) 102-127.