Prevent shoulder surfing using graphical and duo letter authentication

Mr. Kasar Santosh R.,Mr. Baig Arfan J., Mr. Gunjal Vishal S., Mr. Pawar Atul J.,
Prof. Dhokane Rahul M.

Department of Computer Engineering
Shree. Saibaba Institute of Engineering Research and Allied Sciences College, Rahata.
Savitribai Phule Pune University, Pune, India.

ABSTRACT

Generally word-based password are use for the authentication. Graphical password is introduced opposite techniques to word-based passwords. As most users are more familiarized with textual (word-based) passwords than pure graphical password. Shoulder-surfing is a get risk where an attacker can capture a password by direct show or by listening the authentication session. Text can be combined with alphabets, digits, images and or colors to generate session passwords for authentication. Run times password can use only once time because every time a new password is generate. Session Password is support graphical password methods and Pair based methods scheme is both secure and efficient. In this papers, we are propose an improved text-based shoulder surfing resistant graphical password scheme by using graphical and pair based methods is used for alphabets, digits or symbols The user can easily and efficiently login system. Proposed system we have been analyze the security and usability of the proposed methods, and show the supports of the scheme to shoulder surfing and get accidental login.

Keyword: *Secret Pass-Key, Shoulder Surfing, Brute Force Attack, Guessing, Dictionary attacks, Graphical Scheme, Pair Based scheme, Session password.*

---

1. INTRODUCTION

Shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information or password. It is commonly used to obtain passwords, PIN, security codes, and similar data... Graphical passwords is useful authentication method. Which are increasingly used with their small size, compact deployment and underlying cost .The risk of this method like dictionary attack, social engineering and shoulder surfing are define. Random passwords can make the system is easy to use and secure. But the main difficulties of this is remembering in mind or guessing those passwords are easily. The opposites techniques are graphical passwords and pair based. These two techniques has their own drawbacks. Bio-metrics, finger prints, face scan introduced but not generally used. The major disadvantage of this approach is such systems can be costly and the identified process can be slow. But most of them suffering from shoulder surfing which is becoming problem. There are graphical password method that used to support shoulder surfing but it has their own drawbacks is taking more time for the user login.

2. Literature survey

Dhamija and Perrig developed a graphical authentication scheme where the user has to identify the predefined images to prove user authentication. In this system, the user selects a certain number of images from a set of random pictures during registration. Later at the time of login work Introduction related your research work Introduction related your research work the user has to identify the pre-selected images for authentication from set of images.

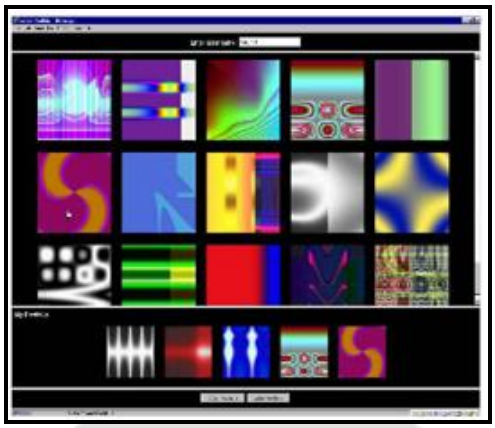

Fig. 2.1 Random images used by Dhamija and Perrig

This system is vulnerable to shoulder-surfing. Pass face is a technique developed by Real User Corporation where the user sees a grid of nine faceprint and selects one faceprint previously chosen by the user as shown in figures. The user recognizes and clicks anywhere on the known faceprints. This procedure is repeated for several rounds. Here, the user chooses four images of human faceprints as their password and the users have to select their pass image from eight other decoy photos. Since there are four user selected photos it is done for four times.
The approach is based on the assumption that people can recall human faceprints easier than other pictures. Pass faceprint is an approach proposed by the Real User Corporation in which the user is allowed to choose four photos of human faceprint from the human photos database as their password security. During the verification phase, the user is provided with a grid of nine faceprint, one already chosen during the registration and eight decoy faceprint. The user identifies the selected faceprint and clicks anywhere over it. This course of action is repeated for four times, and the user is ascertained as genuine if he recognizes all faceprint accurately.

Fig. 2.2 Examples of Pass faces.

To avoid shoulder surfing issues, many design have been proposed. One of such approach is designed by Man, et.al. In this system, the user selects many portraits as the pass objects. Each pass object is allotted an perfect code. During the verification process, the user has to input those exclusive codes of the pass objects in the login interfaces presented by the system. Though the scheme resists the camera, the user has to remind all pass object codes. In this way, many other graphical authentication schemes and their drawbacks are presented in a latest survey paper.

3. DEFINITION

1 Dictionary Attack:

A Dictionary Attacks is a technique used for the defeating a cipher or authentication system by trying to determine its decryption key. It is a method of breaking into a password protected system by systematically enters each word in a dictionary as password.

2 Shoulder Surfing Attack:

It is a password are seeing by looking over a person's shoulder. Both text and graphical password are defenseless.

3 Brute Force Attack:

Brute Force Attack can produce each and every every combination of password.

4 Guessing:

It seems that graphical passwords are often foreseeable, a serious problem typically associated with text-based password.

4. PROPOSED SYSTEM:-

In this study paper we will avoid shoulder surfing and dictionary attacks using two schemes.

1] Graphical based Authentication scheme.
2] Pair based Authentication Scheme.
a) Even Method
b) Odd Method

1] Graphical Authentication scheme:

We will make GUI circle and circle is dividing in 8 equal parts, each part is called as sector. Circle consists of 8 sectors having 8 arcs, each arc has unique color assign and user can be select color at the time of registration.
We will describe a simple shoulder surfing to support graphical password scheme based on alphabets, digits, special symbol and color. The alphabet used in this method contains 64 characters, including 10 digits, 26 upper case letters, 26 lower case letters, and two any type's symbols are used like "#" and "@". Graphical scheme is performing in three phases
1. Registration phase.
2. Login Phase.
3. Verification phase.

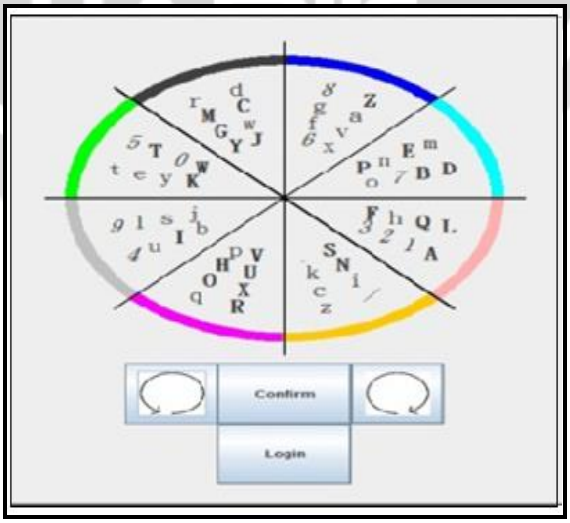

Fig. 4.1 Graphical Login Screen

A. Registration Phase:

User set his password K of length L ($8 \leq L \leq 15$) characters, and choose any favorite color as from 8 colors assigned by the system. The others 7 color not chosen by the user are his blind-color. And, the user has to register an e-mail address for re-modifying his disabled account. The registration phase should proceed in an environment free of shoulder surfing. These data stores the user's word baised password in the user's entry in the password table, which is encrypted by the system key.

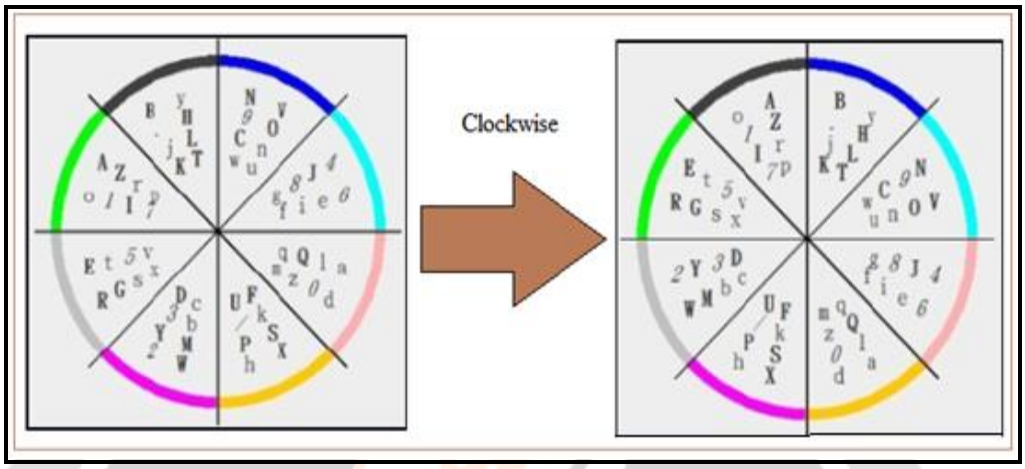

Fig 4.2 Rotation Operation

B. Login phase:

The user requests to the login system, and this system displays a circle of 8 equally divided parts. These parts are called sector. The arcs sectors has different color, and each sector is appropriated by the color of its arc e.g., the pink sector is the sector of pink arc. The 64 characters are placed randomly. All the displayed characters can be concurrently rotated into either the sector rotated clockwise by clicking the "clock-wise" button once or the rotated sector anti-clockwise by pressed the "Anti-clockwise" button, and the rotation operations can also be performed by the mouse using scrolling wheel.

Step 1:

The user requests to the system login.

Step 2:

The system shows a GUI circle composed of 8 equally sectors, and places 64 characters among the 8 sectors. The 64 characters are in three type in that the 26 upper case letters are in bold, the 26 lower case letters and the any type of two symbols "#" and "@" are in regular type, and the 10 digits are in the type. And the button for rotating clockwise and Anti-clockwise, the "Confirm" button, and the "Login" button are displayed on the screen. All the displayed characters can be concurrently rotated "clockwise" OR Anti-clockwise by clicking on the button once, and the rotation operations can also be performed by scrolling the mouse wheel. Let i = 1.

Step 3:

The user has to rotate the sector containing the i^{th} pass-character of his password K, denoted by Ki, into his pass-color sector, and then press the "Confirm" button. Let i = i + 1.

Step 4:

If i< L, the system randomly change the sequence of all the 64 characters displayed, and then GO TO the Step 3. Then the user has to press the "Login" button to complete the login process.

C. Verification Phase:

After successfully of the registration of new user then user can login process to entering User ID and password and check this password is correct or not then perform by verification scheme.

2] Pair Based Scheme:

At the time of registration user can submitted password. Minimum password length is 8 and it can be called as secret key. The secret passkey consisting of even or odd number of characters. Then the login phase, when the user enters his username as an interface. The row and column size 6 x 6 and it consists of capital alphabets and numbers. These are consecutively placed on the grid and these interface change every time. The first letter in the pair is selecting the row and the second letter in the pair is selecting the column. The intersection of that letter click on that letter is part of session password.

1	A	J	R	H	7
0	K	9	I	Q	G
3	B	O	C	P	6
Z	L	4	S	T	2
M	Y	W	D	5	F
8	X	N	V	E	U

Fig. 4.3 Pair Based Scheme

Step 1:

If the password is "SANKITA".

Step 2:

Consider the password selected in the form of pairs.

Step 3:

Searching for the letter which is in the crossing of the pair of the two letters, considering the row of first letter and column of second letter.

5. ALGORITHM USED:-

1. Bresenham's Algorithm:

This is a line drawing algorithm used in computer graphics is Bresenham's Algorithm. This algorithm was introduced to draw lines on plotters, but has found wide-spread uses in computer graphics. It can be implemented with only numerical calculations and very easy to describe. Bresenham's algorithm is used in the Graphical scheme in this scheme circle divided in 8 equal parts is called as sector. Each sector contains 8 letter consists of random combo of number, symbol, upper character, lower character. By using Brenham's algorithm we will put the letter in correct line. It is used in the Graphical Representation.

2. Random Algorithm:

A random algorithm is one of that depends on the random numbers for its operation. Using the random numbers to help find out solution to a problem. The random numbers to improve the solution to a problem. The algorithm is usually simple and easy to implement, fast with very high probability, and it produces an optimum output. We put random letter in the circle and 6 X 6 grid. Analysis of running time or probability of getting an accurate answer is usually difficult. One needs to depend on pseudo random numbers. So, it should be considered as expensive resource like time and space. Thus, one should aim to minimize the use of randomness to extent possible. This assumption describes error and increases the work and the required number of the random bits. There are ways to reduce randomness from several algorithms while maintaining the efficiency nearly the same.

6. ADVANTAGES

A. Easy to register:

In this systems new user register. Then new user can register such as fill the data form such as username, E-mail address, Dob, gender, local address, city, mobile number, password, first name, last name etc.

B. More secure than other:

Textual password scheme are when any user is enter the password then this password seen by other third persons. In textual password scheme passwords should be easy to remember and the easy to cracked. But in graphical and pair-based methods password guessing is not easily done. So it is more secure.

C. Easy to using:

This system is very easy to use because new user can register and use this method.

D. Very hard difficult to hack:

Very little research has been done yet for study the difficulty of cracking graphical passwords. Because graphical passwords are not many times used in practice, there is no report on real cases of breaking graphical passwords. Passwords should be more secure, i.e., they should look random number and should be hard to guess, they should be changed frequently the password, also we avoids so many dictionary attack and this methods are difficult to hack.

7. APPLICATION:-

1. In Companies to store confidential data and all important information with high security.
2. use in the mobile pattern lock
3. In Military for securing confidential data.

8. CONCLUSION:

We have concluded that to avoiding shoulder surfing, dictionary attacks and brute force attack by using this authentication method. The user can easily login the system without using any physical keyboard. We have analyzed the supporting the proposed method to shoulder surfing.

We have proposed a simple word-based shoulder surfing to support graphical password, in which the user can very efficiently and easily complete the login process without any attacks. The operation of the proposed scheme is very simple, easy for learning and easy to use for the users familiarized with textual or word-biased passwords.

9. REFERENCES

[1] Sagar A. Dhanake, Umesh M. Korade and V. M. Lomte, "Authentication Scheme for Session Password using Matrix Color and Text" (IOSR-JCE/ISSN, Jan 2014).

[3] "A Simple Text Based shoulder surfing Resistant Graphical Password scheme" IEEE 2nd International Symposium on Next-Generation Electronics (ISNE), 2013.

[1] Sobrado and J. C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[2] L.Sobrado and J.C. Birget, "Shoulder-surfing resistant graphical passwords," Draft, 2005. (http://clam.rutgers.edu/~birget/grPssw/srgp.pdf.

[4] M Sreelatha , V Manoj Kumar and M Shashi, "Authentication Scheme for Session Password using Color and Images"(IJNSA, May 2011).

[6] Doke Ashvini,Wagh Dhanashree, Shaikh Saddam, "Authentication Scheme for Shoulder surfing using Graphical and Pair Based scheme"(IJARCSMS ISSN: 2321-7782 OCT 2014)

[7] Yi-Lun Chen, Wei-Chi Ku, Yu-Chang Yeh, and Dun-Min Liao, "A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme" IEEE 2nd International Symposium on Next-Generation Electronics (ISNE) - February 25 2013.

[8] M SREELATHA, M SHASHI, V MANOJ KUMAR "Authentication Schemes for Session Passwords using Color and Images " International Journal of Network Security Its Applications (IJNSA), Vol.3, No.3, May 2011.

[9] Bandawane Reshma B., Kumbhar Dnyaneshwar B., "Data Security Using Graphical Password and AES Algorithm for E-mail system" IJEDR | Volume 2, 2014.

[10] Mr. Sagar A. Dhanake, Mr. Umesh M. Korade, Prof. V. M. Lomte "Authentication Scheme for Session Password using matrix Colour and Text" IOSR Jour-al of Computer Engineering (IOSR-JCE) ISSN: 2278-8727 Volume 16, (Jan.2014) //www.iosrjournals.org
[11] VAISHNAVI PANCHAL, CHANDAN P. PATIL. "Authentication schemes for session password" International Journal of Scientific Engineering Research Volume 4, ISSN 2229-5518, March-2013.
[12] N. S. Joshi "Session Passwords Using Grids and Colors for Web Applications and PDA" International Journal of Emerging Technology and Advanced Engineering (ISSN 2250- 2459, ISO 9001:2008 Certified Journal, Volume 3, May 2013) //www.ijetae.com.