Pass Roulette a Text Based shoulder Surfing Resistant Graphical Password Scheme

[1]Ameer H.Abdulsalam, [2]Sawsan k. Thamer

Computer Science Department College of Sciences, Al-Nahrain University, Iraq.

Corresponding author: ameerhussein995@gmail.com

sawsan.kamal@gmail.com

Abstract

Authentication that depends on passwords is for the most part utilized in applications and websites to guarantee protection and security. Users in general select passwords that are either significant or short Rather than subjective alphanumeric strings for simple Remembrance. With web sites and mobile applications heaping up, individuals can get to these applications whenever and wherever with different gadgets. This development brings incredible comfort yet in addition expands the likelihood of passwords being exposed to Shoulder surfing assaults. Assailants can watch straightforwardly or utilize different gadgets to gather user's credentials. To overcome this issue, we proposed an authentication system called Pass roulette which is based on graphical passwords to oppose shoulder surfing attacks. With a 12x2 parts circle and 12 colors with a roulette like system to offer a camouflage, Pass Roulette offers no clue for aggressors to make sense of or limit the secret key regardless of whether they use numerous camera-based assaults.

Keywords: Graphical Passwords, Authentication, Shoulder Surfing Attack, authentication roulette, security

INTRODUCTION

Authentication is generally performed with the assistance of three components – what the user has, what the user is and what the user knows. Passwords are the most primeval type of digital authentication and are broadly used on account of their usability and reliability in comparison to other technologies like smart cards or biometrics. Anyways passwords should be secure (random looking) and easy to recall at the same time, which are two fundamentally conflicting prerequisites. This frequently causing vast majority of people to use anything but secure passwords which are easy to recall and consequently simple to break as well using dictionary attacks or knowledge about the owner of password [1].

Online password authentication is also prone to other attacks like phishing which steal user credentials by impersonating a legitimate person, website or a service. Malicious programs running on the host system like key loggers, bots and other spyware are another attack vector. They record all keystrokes entered and send them to the attacker. They can run as a kernel rootkit and accordingly remain undetectable to anti-virus programs [2].

The human actions for example, picking terrible passwords for their new accounts and using an insecure way of inputting passwords for later logins are viewed as the weakest link in the authentication chain

[3]. Thus, an authentication scheme ought to be made to beat these vulnerabilities.

Authentication systems are generally classified into three categories as shown in Fig. (1)

1. Biometric authentication: behavioral or physiological or features of a person for authentication.

2. Token based authentication: user uses a token to access a specific resource.

3. Knowledge-based authentication: Such as Graphical password and textual password.

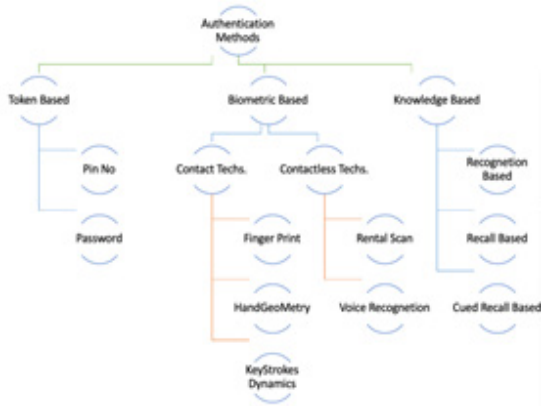

Figure (1): Classification of Authentication methods [2]

Graphical Password

As name demonstrates, graphical password provides different types of shapes and images that's used as password. Graphical passwords can provide advantages regarding the memorability and safety. The memorability advantage could be explained by the effect of pictorial-superiority. The effect of pictorial-superiority is defined is a hypothesis claiming that a person can recall a picture more easily than a text. This hypothesis would also indicate that is a person remembers a graphical password more likely than a textual one [4].

Graphical password systems can be classified in the three categories [5]:

1.Recognition-based Authentication: In Recognition based, different images are exhibited to the user and from that user has to perceive the correct images in the right sequence.

2.Recall-based authentication: in Recall based, user has to imitate something that he/she has made or selected during registration.

3.Hybrid Authentication :it's defined as being a combination of Recognition based and recall based Authentication

Yet, it is observed that graphical password techniques likewise have few limitations and the major limitation known is the vulnerability to shoulder surfing attack as images are utilized as a password. Shoulder surfing implies watching over an individual's shoulder to get the password. At the point uses a keyboard, mouse and touch screen to input password [5].

The proposed procedure is impervious to shoulder surfing to some point and also to other conceivable attacks

RELATED WORK

There is a lot of research work that has been done for graphical password techniques. Graphical password was originally proposed by Blonder in 1996.

Some Examples of Graphical Password Schemes are

1. **Xiyang Liu et al (2011):**

They proposed a novel cued-recall graphical password technique called CBFG utilizing the way of setting password in traditional cued-recall scheme. The technique is for users that tends to make their passwords more complex. Simultaneously, it has the capacity against intersection analysis attack and shoulder surfing attacks. Trials has shown that the CBFG has better performance in usability, particularly in security [6].

2. Hung-Min Sun et al (2016):

It's is an authentication system that's based on graphical password, called Pass Matrix. To resist attacks of Shoulder Surfing, using a one-time valid login indicator, circulative vertical and horizontal bars covering the whole scope, it also doesn't offer hints for attackers[7].

3. Aman Kumar, Naveen Bilandi (2015):

The Proposed system is a combination of recall and recognition based graphical password system that provides great advantages over the existing systems. This system is impervious to shoulder surfing attacks on graphical passwords. This system is made for mobile devices to provide password of higher security [8].

The Proposed system

Like other authentication techniques, the graphical password comprised of two Phases, authentication and registration.

• Registration Phase:

In the registration phase the user needs to set his textual password characters and pick one color as his passing color from 12 colors assigned by the system. The remaining 11 colors (not chosen by the user) are his decoy colors that's used to provide a camouflage for the chosen color. The user needs to register an e-mail address to access his account. The system saves the user's password, email and chosen color in the user's entry in the Database as shown in Fig. (3).

• Login Phase:

At the point when the user requests to login to the system, and the system displays a circle composed of 12 similarly sized segments. The colors 12 segments are different, and each segment is identified by a color. At first, 24 characters are placed averagely and haphazardly among these sectors. All the Sectors can be at the same time rotated either clockwise by clicking the "clockwise" button once or counter clockwise by clicking the "anti-clockwise" button once and every time the user selects a character all the characters of all the sectors will be shuffled.

As shown in Fig. (2) the alphabet used in the proposed scheme composed of 24 characters (including all lower-case characters & numbers) divided across 12 sections, each section contains 2 orbits, first one called outer, the second one (confined in the black circle) is called inner orbit.

FIGURE (2):Pass Roulette overview

The authentication process of this scheme begins by retrieving password and chosen color depending on user's email that he used during registration from the database, after that the user will use the roulette facility to rotate the circle to sync between the chosen color and the chosen character, after that he will have to select the characters in the outer and inner orbit and then compare it with the one saved in database as shown in the following flowchart Fig. (3).

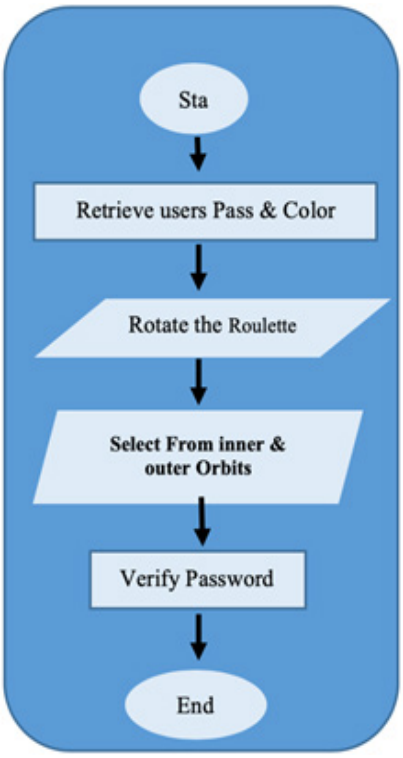

Figure (3): Block Diagram of the Authentication Process

Advantages:

• Allows users to log into their account more safely.

• Assailants will not be able to record the password via shoulder surfing.

• Complex password technique with simple user interface.

Disadvantages:

• If user forgot password color, then he/she must enter the password for each of the 12 colors.

SYSTEM IMPLEMENTATION

System implementation is comprised of three steps begins with Creating the circle and ends with verifying the entered password with the one saved in database during registration.

When the user opens the application, he or she will be presented with a two buttons: registration and login. Pressing the Registration button will take the user to the registration process, the user will be sent back to the menu once the registration is completed. Pressing the login button will take the user to the authentication process where he or she will go through the login procedure with the registered password.

1. Circle creation

In this Method a 12 Parts Circle is Created, the full Circle Contains 24 Character which Represent the full range of available characters, each Parts Contains 2 characters and also each part contains a color that's related to the selected user color.

Algorithm (4.1): Roulette circle creation Output:The roulette circle
Steps: Step 1:Create 12 parts from 1 to 12 Step2:Rotate each art by : 0°,30°,90°,120°,150°,180°,210°,240°, 270°,300°,330° accordingly. Step 3:Skew each of the 12 parts by -60° Step4:For Each item put its Color To one of the default colors Which are green, tomato, aqua, yellow, orange, purple etc.

Algorithm (4.2): creating inner and outer orbits. Input: the previously created items Output: furtherly segmented circle
Steps: Step1: Input (read) list of items (1-12)item Step2: using div class, divide each class (item) into two (sub classes) child classes. Step3: assign an id to each child class (subclass). Step4: end.

2. Circle parts division

To increase the security of this scheme and range of usable range of characters, each part of the 12 ones will be divided into two orbits (inner and outer) each orbit contains one value that differs from the value of other orbit that belongs to the same part of the circle, these orbits called inner and outer orbit.

3. Circle rotation

In order to provide Shoulder Surfing prevention facility, the circle should be rotated so that the characters and colors will be changed So that only legit user will be able to figure out the selected color and after that he should chose the correct character form inner and outer orbits.

SYSTEM RESULTS AND DISCUSSION

The proposed roulette system has been evaluated in terms of password space, accidental logins and shoulder surfing protection using recorded videos or key logger.

1. Password Space

The proposed System uses a set of 24 character, these characters are similarly and arbitrarily partitioned among 12 parts and password length L is in range of ($8 \leq L \leq 20$). Accordingly the maximum number of possible passwords of length L is 24L. Subsequently the password space of the proposed system is given by,

$$P_s = \sum_{L=8}^{20} 24^L = \approx 1.391724288887253e^{+27}$$

2. Accidental Logins

The probability of an attacker login to accidently being correct can be measured by dividing the number of characters to the number of sectors and in my case it's (12/24) i.e. (1/2) and then multiply by power to length of password so the equation would be for L=10:

Pal (12) = (1/2)12 = ≈0.00024414062

(2)

3. Usability

As most user think about textual passwords, it's commonly less demanding for the user to detect character than symbols when using the login screen. Since the system uses letters and numbers on the login screen, the user without a lot of stretch professionally discover his chosen password. Furthermore, the operation of the proposed system is simple and basic for the user to log in, he just needs spin the divisions correctly.

4. performance

In table (1), data were collected based on the mean login time, the mean success login percentage. We also recorded the length of password and the number of logins. The experimental data are shown in Table 1 (in which PL means Length of password, LC means length of password, LMT means login mean time, SR means Success rate

Table 1 System Test Data

ID	LC	PL	LMT	SR
PT1	4	8	30	100
PT2	2	10	25	100
PT3	3	9	30	100
PT4	2	10	32	100
PT5	4	8	21	100
PT6	3	9	30	100
PT7	2	10	30	100
PT8	2	12	36	100

part from regular shoulder surfing which include a person watching your password entry, after testing the scheme on 5 personals, and performing three login sessions for each user and then recording the sessions there was no similarity in character distribution among the sessions for each user, there for the similarity of shoulder surfing chances to succeed are close to zero.

CONCLUSION AND FUTURE WORK

The proposed system is a Textual based graphical password approach created for shoulder surfing elimination. Also, it offers more security and usability compared to former graphical password authentication systems. The password space is very large it provides optimum security against brute force attack. It is easy to use. Passwords can be created and be memorized easily.

The proposed graphical password scheme eliminates shoulder-surfing attacks involving recording more than one session because in each try the user's password and camouflage password in the inner and outer orbits are shuffled together so that each time the color indicator will point to different part of the circle. Generally speaking this system is impervious to most conceivable attacks also. This system can be utilized for highly secure systems.

REFERENCES

[1] S. Brostoff, and M. A. Sasse. "Are Passfaces more usable than passwords? A field trial investigation." People and Computers XIV— Usability or Else!. Springer London, 2000. 405-424.

[2] C. Herley, and D. Florencio. "How to login from an Internet café Without worrying about keyloggers." Symposium on Usable Privy and Security (SOUPS). Vol. 6. 2006.

[3] M. Sasse, S. Brostoff, and D. Weirich, "Transforming the weakest linka human/computer interaction approach to usable and effective security," BT technology journal, vol. 19, no. 3, pp. 122–131, 2001.

[4] Whitehouse, A., Maybery, M., and Durkin, K., "The development of the picture-superiority effect," British Journal of Developmental Psychology, vol. 24, no. 4, pp. 767–773, 2008.

[5] Elias Alesand and Hanna Sterneling,"A shoulder-surfing resistant graphical password system" Linköping University, 2017

[6] JinhuaQiu, Xiyang Liu, Licheng Ma, Haichang Gao and ZhongjieRen,A Novel Cued-recall Graphical password Scheme, International Conference on Image and Graphics page949956, Washington,2011.

[7] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng," A Shoulder Surfing Resistant Graphical Authentication System", TDSC, 2016.

[8] Aman Kumar, Naveen Bilandi,"a graphical password based authentication based system for mobile devices", JCSMC, vol.3, 2015