Journal of Engineering Sciences

Vol 11, Issue 3, March/2020
ISSN NO:0377-9254

TEXT-BASED SHOULDER SURFING AND KEY LOGGER RESISTANT GRAPHICAL PASSWORD

NEERUKONDA JITENDRA[1], NELLURI SAI VINAY[2], PALUKURI SRI RAM[3],
PUTHUMBAKA NAGA SIDHARDHA[4], D. DEEPTHI[5]
[1,2,3,4]B. Tech Student, [5]Assistant Professor,
Department of CSE,
VASIREDDY VENKATADRI INSTITUTE OF TECHNOLOGY, A.P., India.

ABSTRACT: The conventional password schemes are vulnerable to shoulder surfing and keyloggers. To overcome this problem many other authentication systems like token-based authentication, biometric based authentication systems, graphical password schemes have been proposed. However, biometric based authentication systems are costly and graphical password systems are not that secure and efficient. As most users are more familiar with textual passwords than pure graphical passwords, text-based graphical password schemes have been proposed. Unfortunately, none of existing text-based shoulder surfing resistant graphical password schemes is both secure and efficient enough. In this project, we propose an improved text-based shoulder surfing resistant graphical password scheme by using colors. A shoulder-surfing attack consists of a user being filmed or watching from behind the shoulder during his/her login. A keylogger is a type of surveillance technology used to monitor and record each keystroke typed on a specific computers keyboard. The user can easily and efficiently to login the system without using any physical keyboard or on-screen keyboard. It will describe a simple and efficient shoulder surfing resistant graphical password scheme based on texts and colors.

Keywords: shoulder surfing, keyloggers, authentication.

INTRODUCTION

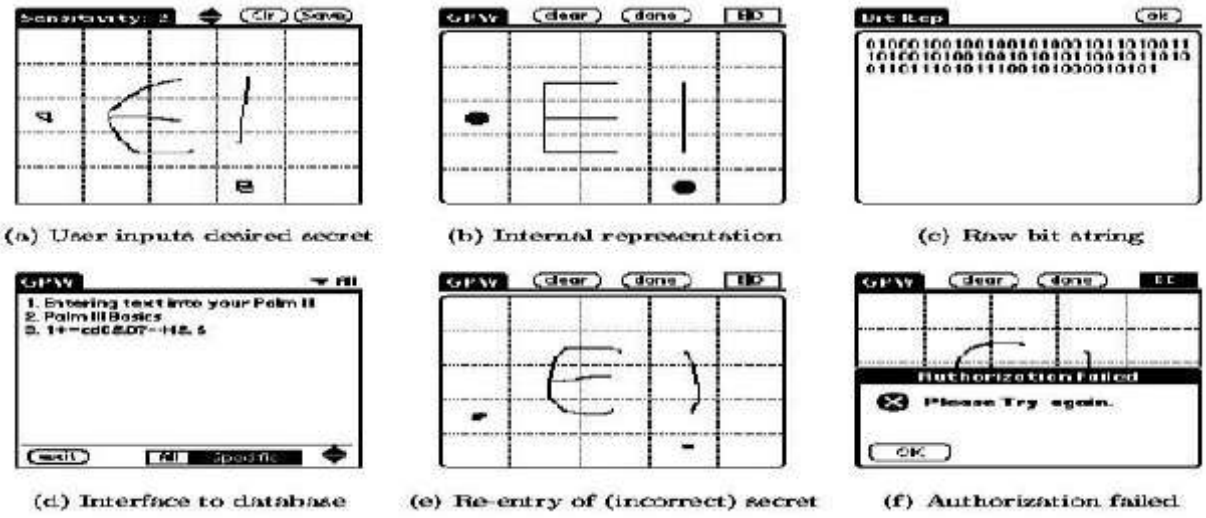
Keylogging is the practice of noting the keys struck on a keyboard, typically in a manner so that person using the keyboard is unaware that such action is monitored. There are two types of keyloggers viz. software keylogger and hardware keylogger. Software keylogger are installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded. Hardware keyloggers are small hardware devices. These are connected to the PC and/or to the keyboard and saves every keystroke into the file or in the memory of the hardware device. Many authentication systems are invented to avoid problem of keyloggers and shoulder surfing for e.g. biometric systems. Shoulder surfing is a technique of gathering information such as usernames and passwords by watching over a person's shoulder while he/she logins into the system. Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. If the code match, the process will be completed and the user will be authorized for access. Traditionally, alphanumeric passwords have been used for authentication, but they are known to have security and usability problems. Now day's graphical passwords are other alternatives. The passwords require the following fundamentally requirements so that the problems with passwords arises. (a) Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans. (b) Passwords should be secure, i.e. they should be different and should be difficult to guess.

LITERATURE SURVEY

Today, password is the most popular way to authenticate a user to login to computer systems. However, we all know that traditional text-based password systems are vulnerable to the shoulder-surfing and keylogger attack. To overcome this problem various solutions came into picture respectively:

- **DAS(Draw-a-Secret)**

In 1999, **Germyn** proposed DAS scheme in which a password is a simple picture drawn on a two-dimensional grid. The co-ordinates of the grids in which the picture touched are recorded in temporal order of the drawing. It gives the user certain degree of freedom to tolerance their drawing during login process. As long as same cells are crossed with same order, a user is authenticated.
It is a Recall based technique.



(a) User inputs desired secret (b) Internal representation (c) Raw bit string

(d) Interface to database (e) Re-entry of (incorrect) secret (f) Authorization failed

- In 2002, **Sobrado and Birget** proposed three shoulder surfing resistant graphical password schemes

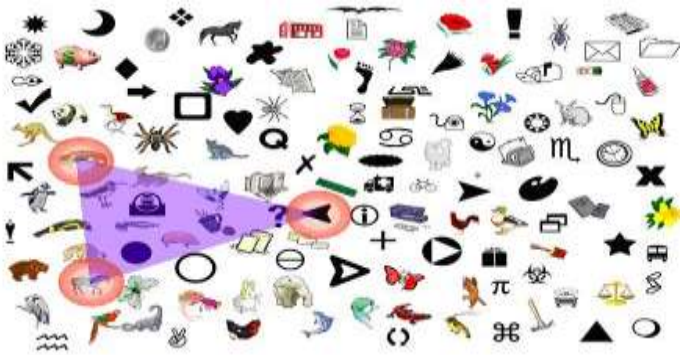
  o The Intersection scheme
  o The Movable Frame scheme o The
  Triangle Scheme

  It is Recognition based technique.

  In Movable frame password scheme user's picture password is located in the frame user have to create an invisible straight line that connect entire picture password. In Intersection scheme user has to intersect all the pass images. Both of these schemes have high failure rate.

Movable Scheme Intersection scheme

In the Triangle scheme, the user has to choose and memorize several pass icons as his password. Every time the user has to login, he has to find three pass icons among a set of randomly chosen icons displayed on the login screen. Then he has to click inside the invisible triangle created by those three pass icons.



- In 1996, **Blonder** proposed a graphical password scheme in which user has to create his password by clicking on various locations on an image. While login into the system user must click on the approximate areas of those location.

- In 2005, **Pass fa**ce is a technique developed by Real User Corporation based on the assumption that people can recall human faces easier than other pictures. The basic idea is as follows. The user is asked to choose four images of human faces from a face database as their future password. In the authentication stage, a grid of nine faces is presented to the user, having eight decoy faces and one face previously chosen by the user. The user memorizes and recognizes the face and clicks anywhere on the known face. Repetition of this process happens for several rounds. On correctly identifying all the faces, the user is noted as an authenticated user.

- In 2009, **Gao** proposed a shoulder surfing resistant graphical password scheme, Color Login, in which the background color is a usable factor for reducing the login time. However, the probability of accidental login of Color Login is too high and the password space is too small.

As most users are familiar with textual passwords and conventional textual password authentication schemes have no shoulder surfing resistance.

- In 2007, **Zhao** proposed a text-based shoulder surfing resistant graphical password scheme, known as S3PAS, in which the user finds his textual password and mixes his textual password to get a session password for login. However, the login process of Zhao scheme is complex and tedious.

- In 2011, **Sreelatha** also proposed a text-based shoulder surfing resistant graphical password scheme by using different colors. The user has to keep in mind the order of various colors, which puts burden on user memory.

- In 2012, **M.K Rao** proposed a text-based shoulder surfing resistant graphical password scheme, known as PPC to login. The user has to mix his textual password in order to create various pass-pairs. After this to get his session password on the login screen follow four predefined rules. But the login process of PPC is too complicated and tedious.

Techniques	Usability		Security issues
	Authentication process	Memorability	Password Space
Text-based password	Type in password, can be very fast	Depends on the password. Long and random passwords are hard to remember	94^K (there are 94 printable characters excluding SPACE, N is the length of the password). The actual password space is usually much smaller.
Sobrado and Birget	Click within an area bounded by pre-registered picture objects, can be very Fast	Can be hard to remember when large numbers of objects are involved.	N!/K!(N-K)! (N is the total number of picture objects; K is the number of pre-registered objects)
Passface	Recognize and pick the pre-registered pictures; takes longer than text-based password	Faces are easier to remember, but the choices are still predictable	N^K (K is the number of rounds of authentication, N is the total number of pictures at each round)
Germyn	Users draw something on a 2D grid	Depends on what users draw. User studies showed the drawing sequence is hard to remember	Password space is larger than text based password. But the size of DAS password space decreases significantly with fewer strokes for a fixed password length
Blonder	Click on several pre registered locations of a picture in the right sequence	Can be Hard to remember	N^K (N is the number of pixels; K is number of locations to be clicked on)
M K Rao	User familiarity with text interface User training required for graphical interface.	User has to remember the rules. Longer Login time than above Scheme.	Password space is same as textual password
Gao	Click on pre-registered pass icons of the color selected during registration	Can be hard to remember	Password space is too small

PROPOSED SYSTEM

In this, section, a simple and efficient shoulder surfing resistant and keylogger resistant graphical password scheme based on text and sectors is described. The user can choose his password from 72-character set. The character set is consisting of 26 lower case(a-z) alphabets, 26 upper case(A-Z) alphabets, 10 decimal digits (0-9) and 10 special symbols (.,/,!, @, #, $, %,^,&,*). In proposed system, login screen is consisting of a circle and that circle is divided into eight sectors, all the 72 characters are equally and randomly distributed among these eight sectors.

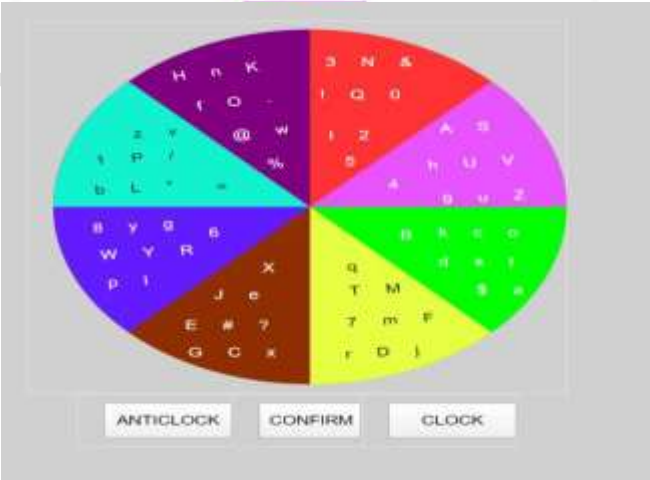
The proposed scheme involves Registration and Login phase

Registration Phase

In the proposed scheme user has to set textual password. The minimum length of Password is 8 Characters and the maximum length of password is 15 characters i.e. password length is between 8 to 15 Characters, and choose one color as his pass color from 8 colors assigned by the system. And, the user has to register an e-mail address and phone number for reenabling his account when he enters a wrong password. In this scheme, registration process should carry out in an environment free of shoulder surfing. So, in short in registration phase the user set is textual password and select 1 Color from 8 Colors.

Login Phase

In the login phase when an user sends an login request to the system, the system displays a circle which is composed of 8 sectors of equal size. The colors of the arcs of each sector is different, and every sector is identified by the color of its arc. In this step 72 characters are placed equally and randomly among these sectors. All the displayed characters can be simultaneously rotated into either the adjacent sector clockwise by clicking the" clockwise" button once or the adjacent sector Anti clockwise by clicking the" Anti clockwise" button once, and the rotation operations can also be performed by scrolling the mouse wheel.



Algorithm:

To login the system user has to finish following steps.

Step 1: The user request to login the system.

Step 2: The login screen displays a circle composed of 8 equally sized sectors, and places 72 characters among the 8 sectors randomly such that each sector contains 9 characters. In addition, the button for rotating clockwise, the button for rotating anticlockwise, the "Confirm button", are displayed on login screen. All the displayed characters can be simultaneously rotated into either the adjacent sector clockwise by clicking "clockwise" button or adjacent sector anticlockwise by clicking "anticlockwise" button once, and rotation operation can also be performed by using mouse wheel.

Step 3: The user has to rotate the sector containing the i-th pass character of his password K, denoted by Ki, into his designated sector, and then clicks the "Confirm" button.
Let i= i+1.

Step 4: If i<L, the system randomly permutes all the 72 characters, and then goes to step 3. Otherwise, user has to click the login button to complete log in process.

The account will be disabled, if the account is not successfully authenticated for two consecutive times. In such case, an email containing ten alpha numeric characters will be sent to user which can be used for re-enable his disabled account.

After successfully authenticating the person through the above proposed method for providing additional security OTP is sent to user registered mobile, which he has to enter for completing the login process.

ANALYSIS

The analysis of the proposed system is done in this section on the basis of usability and security.

Password space

The proposed system has character set of 72 characters, these characters are equally and randomly divided among 8 sectors and password length L is in between 7<L<16. Therefore total number of all possible password with length L is $8*72^L$. therefore, password space of proposed scheme is given by,

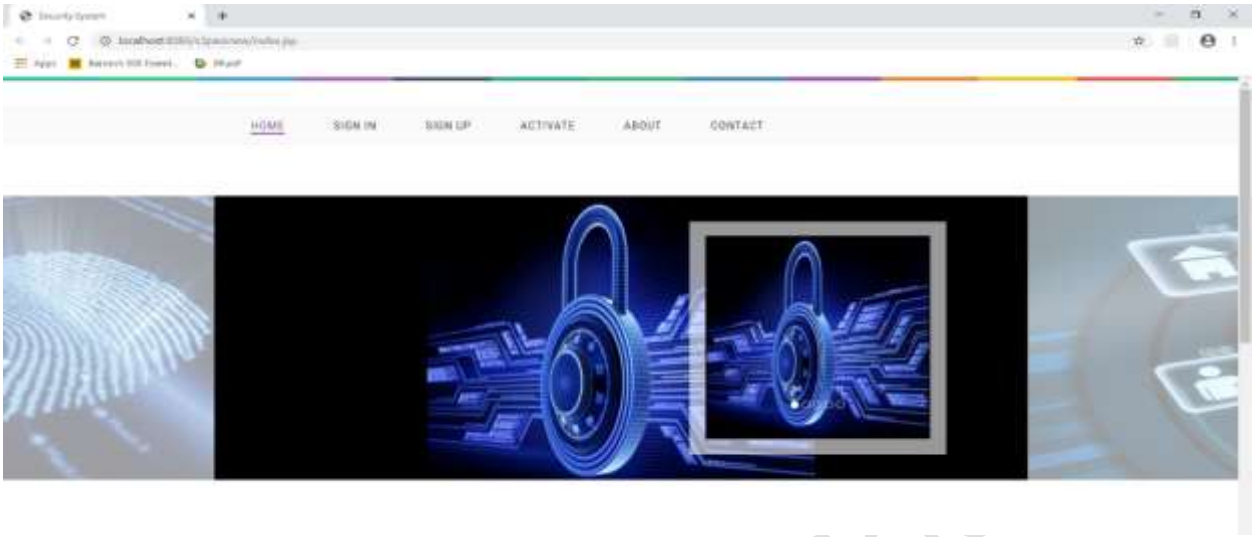
$$\sum_{L=8}^{15} 8 * 72^L$$

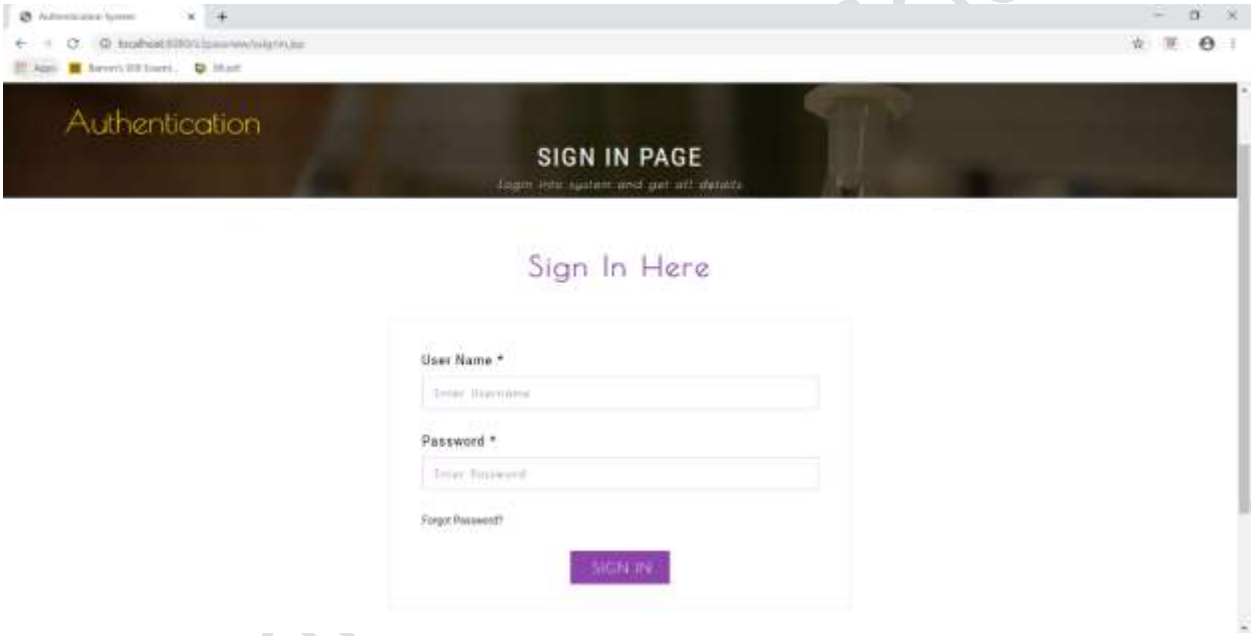
Resistant to accidental login

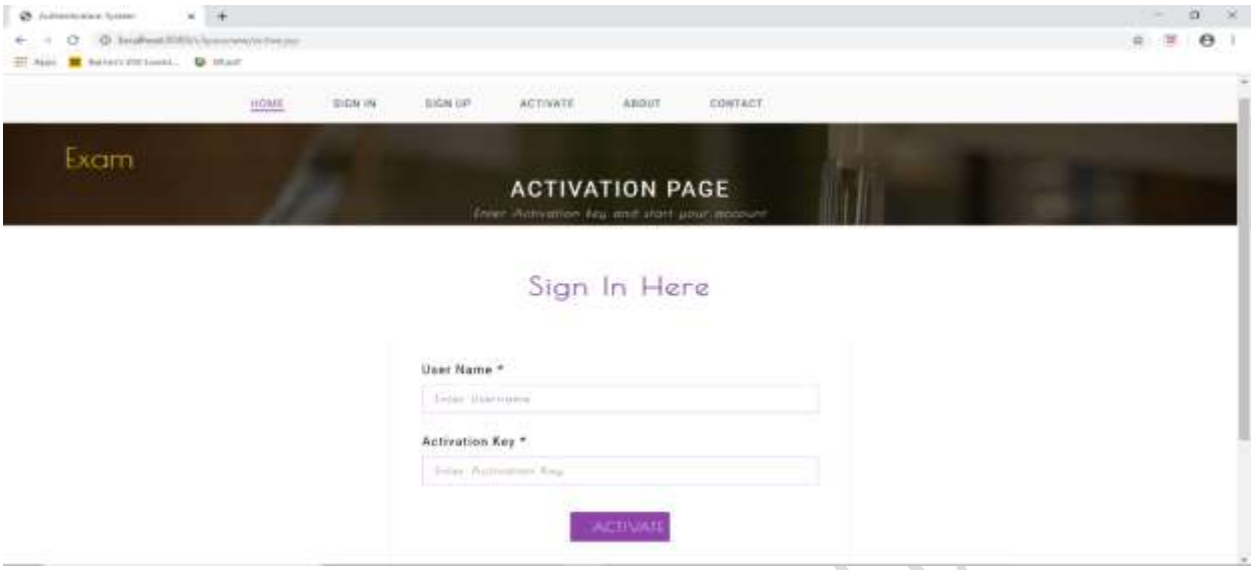
Since the probability of correctly responding to Ki is 8/72 i.e. 1/9. The success probability of accidental login with the password length L denote by $P_{al(L)}$, is

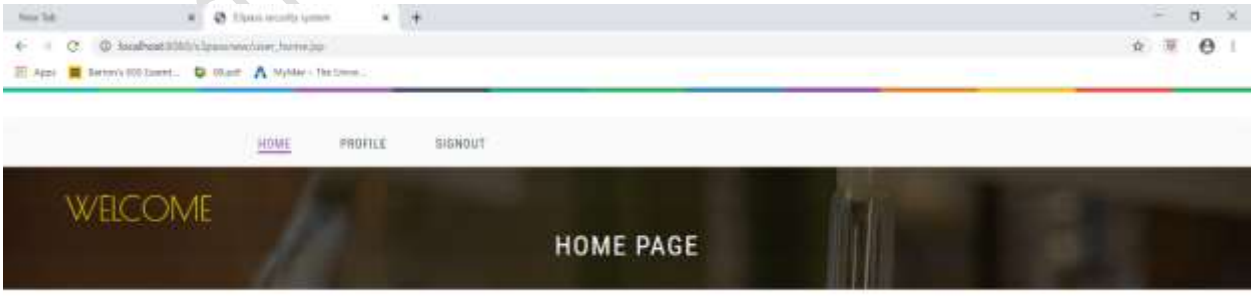
$$P_{al(L)}=(1/9)^L$$

SAMPLE RESULTS


HOME
SIGN IN
SIGN UP
ACTIVATE
ABOUT
CONTACT


Authentication
SIGN IN PAGE
Sign In Here
User Name *
Password *
Forgot Password?
SIGN IN





You are successfully Login

Jitendra

CONCLUSION

In this paper, analyse the key logger resistant text-based graphical password scheme is proposed. The working of the proposed scheme is easy to learn for users familiar with textual passwords. In this system user can easily login into system without worrying about shoulder surfing and key logger attack. User just have to remember pass sector and alphanumeric password. This scheme is simple and efficient. Unlike other graphical password scheme user can easily log into the system without remembering graphical sequences. This system do not need use of physical or on-screen keyboard. Finally, we have analysed the resistances of the proposed scheme to shoulder surfing and accidental login.

REFERENCES

[1] Germyn, A. Mayer, F. Monrose, M. Reiter and A. Rubin. The design and analysis of graphical passwords. In Proceedings of the 8th USENIX Security Symposium, August 1999.

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

[3] G. E. Blonder. Graphical passwords. United States Patent 5559961, 1996.

[4] R. U. Corporation. How the pass face system works, 2005.

[5] H. Gao, X. Liu, S. Wang, H. Liu, and R. Dai, "Design and Analysis of a graphical password scheme," Proc. Of 4th Int. Conf. On Innovative Computing, Information and Control, Dec. 2009, pp.675-678.

[6] H. Zhao and X. Li,"S3PAS: A Scalable shoulder-surfing resistant textual-graphical password authentication scheme" Proc. Of 21st Int. Conf. On Advanced Information Networking and Applications Workshops, vol. 2, May 2007, pp467-472.

[7] M. Sreelatha, M. Shashi, M. Anirudh, Md. Sultan Ahamer, and V. Manoj Kumar "Authentication schemes for session passwords using color and images," International Journal of Network Security &Its Application, Vol. 3, no 3,May 2011.

[8] M. K. Rao and S. Yalamanchili. "Novel shoulder-surfing resistant authentication schemes using text-graphical passwords," International Journal of Information & Network Security, vol. 1, no. 3, pp. 163-170, Aug. 2012.