Asian Journal of Science and Applied Technology
ISSN: 2249-0698 Vol. 6 No. 1, 2017, pp.42-45

An Efficient Graphical Authentication System

Aayush Kumar[1], Keshav Kumar[2], Siddharth Shekhar Singh[3] and M. Vaneeta[4]
Department of CSE, K.S Institute of Technology, Bangalore, Karnataka, India
E-Mail: aayushkumar.poddar@gmail.com, keshavraj243@gmail.com
siddharth.shekhar08@outlook.com, vanitamss@gmail.com

Abstract **- Password authentication is majorly used in applications for computer security and privacy. However, human actions such as selecting bad passwords and inputting passwords in an insecure way are considered as" the weakest link" in the authentication process. Rather than arbitrary alphanumeric string, users generally use weak password, more often based on their personal information. With new technologies coming up and mobile apps piling up, users can use the application anytime and anywhere with various devices. Although the evolution is convenient but it also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' credentials. To overcome this problem, a novel authentication system Pass Matrix, based on graphical passwords is proposed to resist shoulder surfing attacks. With a one-time code and horizontal and vertical bars covering the entire scope of pass-images, Pass Matrix will offer no hint to attackers to figure out or narrow down the password even they conduct multiple camera-based attacks. We will implement a Pass Matrix prototype and from the experimental result, the proposed system will achieve better resistance to shoulder surfing attacks while maintaining usability**

Keyword: **Graphical Passwords, Authentication, Shoulder, Surfing, Attack.**

I. INTRODUCTION

Human factors are considered as weakest link in password authentication system. In general, we choose to keep password on our personal information which is easy to guess by our friends. Technically speaking, in recent years, information security has been considered as an important problem. Main area of information security is authentication which is the determination of whether a user should be allowed access to a given system or resource. In this context, the password is a common and widely authentication method.

The most common computer authentication method is for a user to submit a user name and a text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember.

Unfortunately, these passwords can also be easily guessed or broken.

Other limitations of normal passwords are hacked password, forgetting password and stolen password [1]. Therefore, strong authentication is needed to secure all our applications. Ordinary passwords have been used for verifiability but they are known to have problems in usability and security. Recent days, another method such as graphical authentication is introduced. Graphical password has been proposed as an alternative to alphanumeric password. Psychological studies have shown that people can remember images better than text. Images are generally easier to be remembered than alphabets and numbers, especially photos, which are even easier to be remembered than random pictures.

II. RELATED WORK

In the past several decades, a lot of research on password authentication has been done in the literature. Among all of these proposed schemes, this paper focuses mainly on the graphical-based authentication systems. To keep this paper concise, we will give a brief review of the most related schemes that were mentioned in the previous section. Many other schemes such as those in may have good usability, they are not graphical-based and need additional support from extra hardware such as audio, multi-touch monitor, vibration sensor, or gyroscope, etc. In the early days, the graphical capability of handheld devices was weak; the colour and pixel it could show was limited. There are several algorithms (recognition based algorithms, recall based algorithms, hybrid algorithms) which were used for authentication for graphical passwords. The brief information followed by their drawbacks of some of the algorithms are given below:

A. Pass Faces

Brost off proposed Pass Faces [2], which is motivated by the fact that humans are familiar with the faces. In this system, users need to click on face images which are already selected in registration for several attempts. However, it has some serious security problems. Pass Faces is vulnerable to shoulder surfing attacks and spyware because face images are clearly shown. Guessing attack is high with few authentication rounds as the probability of detecting correct faces is high. Also, there are some predictable images which users are more likely to select based on race, complexion and gender.

B. The Draw-A-Secret (DAS) Scheme

An entirely graphical password and input scheme was used in this system, which we call "Draw-A-Secret". This approach is alphabet independent, thus making it equally accessible for speakers of any language. Users are freed from having to remember any kind of alphanumeric string. But in the case of the DAS scheme, similar assumptions about user choice do not exist. Furthermore, the learning task is made even more difficult by two factors. First, the space of passwords and the space of likely user choices are considerably larger than for textual passwords. Second, the platform that we are targeting, PDAs, renders the task of data collection much harder than on, e.g., networked computers.

C. DejaVu

Déjà vu [3] was proposed by Dhamija, where users select a specific number of random art images from a set of images generated by a program in the registration phase. At the time of authentication, the system shows a set of images that contains both password images and decoy images. The user has to identify the password pictures from the challenge set of password images and decoy images. It is easy to store and transmit the random art images generated by small initial seeds and also the art images make it inconvenient to record or share with others. This system has several drawbacks such as hard to remember an obscure picture and the corpus size is much smaller than that of text based passwords.

D. Pass Faces

Story Another recognition based scheme, Story [4] which is similar to PassFaces only needs one round of authentication, but password pictures are a sequence of number of unique images that makes a story to enhance memorability. When users authenticate, users have to click the password pictures. The story needs the users to remember the order of images.

So, it makes the users difficult who are not using a story to guide the image selection to memorize the password. Studies show that, of the all incorrect password entries in Story, over 80% of them contained all the correct images, but with incorrect order. Therefore, the importance to "make a story" should be emphasized to users.

E. Graphical Passwords with Icons

Graphical Password with Icons (GPI) [5] is designed aimed at solving the hotspot problem. In GPI, users select 6 icons from 150 icons as a password in one panel. With GPIS, the system generates a random password and displays it to users. If the user is not satisfied with the password the system generated, he can request the system generate new password until accepted. The main drawback of GPS is its unacceptable login time and small size of icons.

F. Cognitive Authentication Cognitive Authentication

[6] is another recognition based algorithm designed to resist shoulder-surfing and spyware. If a user stands on an image belonging to the portfolio, then the user will move right or move down until the bottom or right edge of the panel is reached, the label of column or row is stored and a multiple choices question which includes the label for the correct point of the path is displayed for each round. Cognitive authentication system computes the cumulative probability of the correct answer to ensure that was not entered by chance after each round. When probability is above a certain threshold, authentication is success. Threshold value enables the system to tolerate user errors up to some extent. An observer who stores any feasible number of successful authentication sessions cannot recover the user's password by the conjectured brute-force or enumeration method.

III. METHODOLOGY

A. User Registration

In this module user has to register by giving his information such as user id, user name, password valid e-mail id etc, and after giving this information, randomly three images will be assigned to the user, in those images he has to select the coordinate squares of the images as the graphical password. The details of coordinates of all images will be stored in the database with respect to the specific user.

B. Hash code generation

After successful setting of the coordinates of the images those details will be stored in the database, concatenating all the three images coordinates and generate hash code for that and store in the database with respect to the user.

C. User Login Process

Registered user will be login to the application by using his user id and password, if the user id and password is valid One Time Password(OTP) will be sent to the user's e-mail, whereas OTP contains the random pair of vertical and horizontal slider coordinate points of all the three images. After successful login three assigned images will be displayed to the user with horizontal and vertical sliders user has to set the horizontal and vertical sliders for all the three images where the OTP coordinate value should be equal to the coordinates chosen by the user at the time of password setting. The hash code will be generated for all OTP coordinates by concatenating if the hash code is matched with the existing hash code user can successful enter in to the home page else, process ends and login page will display.

D. Admin

Admin has to login to his account by the authenticated user name and password. Admin can able to view all the users details, who are successfully registered.

IV. IMPLEMENTATION

1. Click Based Image Co-ordinate Generation
2. Password String creation & Secret Code generation
3. One Time Code (OTC) Generation
4. OTC Verification
5. Scroll Bar based Image Co-ordinate Generation
6. Secret code Comparison.

A. Randomized Image Selection Algorithm

This algorithm is invoked when user is registered with our system for each user our system has to pick 3 distinct random images from Password image database for this purpose this algorithm is used.

B. Click Based Pixel to Co-ordinate conversion

When a user clicks on the image x and y co-ordinate pixel he retrieved. These pixel location has to convert into column offset, row offset coordinates which makes user friendly selection process

.

C. Password string creation

As per the system user has to select 3 locations on 3 images (1 location per image). Using previous algorithm the pixel location converted into co-ordinate. Concatenating all the coordinates we get a password string. By using hashing technique on generate password string system produce secret hash code which has to stored in database for password verification.

D. One Time Code (OTC) Generation & Email Sending

There is a different between OTC and OTP. OTP is one time password which act as a password itself, OTC one time code it is not a password, it a clue for the user to select password image co-ordinate, this algorithm is used to generate OTC.

E. OTC & Scroll Bar Mapping and Co-ordinate Generation

Once the user receives the OTC he has to move the vertical scrollbar and horizontal scroll bar on password image to point the co-ordinate. We need the system based on scroll bar movement co-ordinates has to be generated.

F. Secret code comparison

Once co-ordinates are generated the hash code has to be extracted on the co-ordinate string. The extracted hash code verified with secret hash code which is stored in data base. If both are same this algorithm allow the user to login home page

.

V. RESULTS

A. Home Page

This is the first page, index page(say) of t project. This figure depicts the interface of login of admin and login and registeration of user.

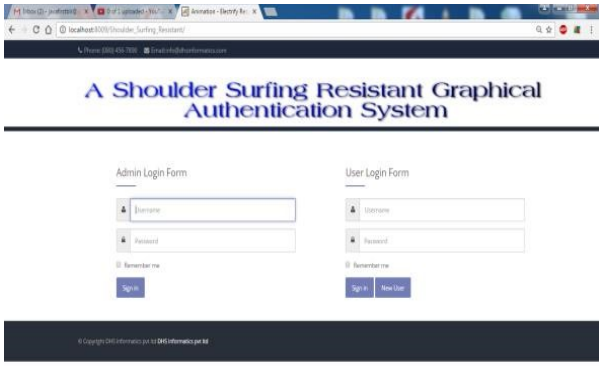

Fig. 1 Home Page

B. New User Registration

Here user can register giving his details as per the requirement of the account.

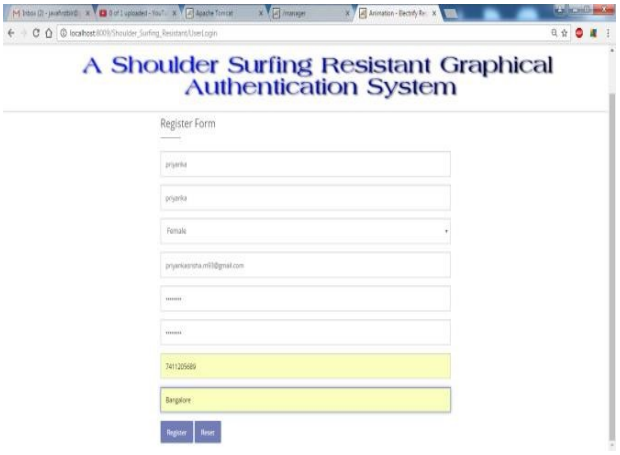

Fig. 2 New User Registration

C. Image password settings

This the part of User Registration process, wherein user is asked to select co-ordinates from randomly generated images.

Fig. 3 Image

Similarly there will be two more images randomly generated by the server.

D. OTC from mail

After successful user registration, users can login for which they will get a code on mail and text message as well.
Here is the image regarding OTC from mail.

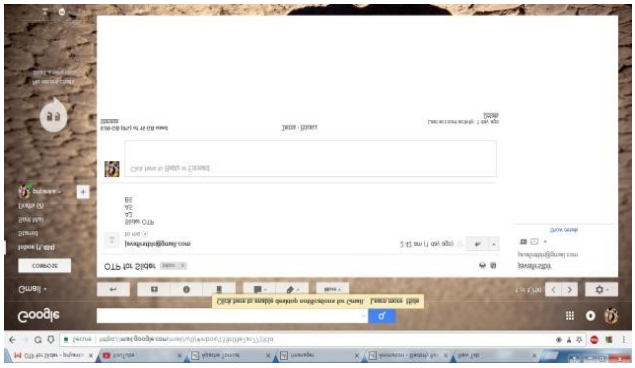

Fig. 4 OTC

E.Rearranging the coordinates

Finally, our expected output that is to slide the horizontal and vertical bars according to the OTC received is done.

Fig. 5 Rearranging the coordinates

VI. CONCLUSION

With the increasing trend of web services and apps, users are able to access these applications anytime and anywhere with various devices. However, conducting the authentication process in public might result in potential shoulder surfing attacks. Even a complicated password can be cracked easily through shoulder surfing. Using traditional textual passwords or PIN method, users need to type their passwords to authenticate themselves and thus these passwords can be revealed easily if someone peeks over shoulder or uses video recording devices such as cell phones.

To overcome this problem, we proposed a shoulder surfing resistant authentication system based on graphical passwords, named Pass Matrix. Using a one-time login indicator per image, users can point out the location of their pass-square vulnerable to shoulder surfing attacks. Because of the design without directly clicking or touching it, which is an action of the horizontal and vertical bars that cover the entire pass image, it offers no clue for attackers to narrow down the password space even if they have more than one login records of that account.

ACKNOWLEDGMENT

Authors would like to thank VGST (Vision Group on Science and Technology), Government of Karnataka, India for providing infrastructure facilities through the K-FIST Level I project at KSIT, CSE R&D Department, Bengaluru.

REFERENCES

[1] Phen-Lan Lin, Li-Tung Weng and Po-Whei Huang,“Graphical passwords using images with random tracks of geometric shapes,” 2008 Congress on Images and Signal Processing. 2008.
[2] Sacha Brostoff, M. Angela Sasse, “Are Passfaces More Usable Than Passwords? A Field Trial Investigation, 2000.
[3] Dhamija R. and Perrig A., “Déjà vu: A User Study Using Images for Authentication”, in Proceedings of 9th USENIX Security Symposium, 2000.
[4] Davis, F. Monrose, and M. K. Reiter, “On user choice in graphical password schemes”, in Proceedings of the 13th Usenix Security Symposium. San Diego, CA, 2004.
[5] K. Bicakci, N. B. Atalay, M. Yuceel, H. Gurbaslarand B. Erdeniz, “Towards usable solutions to graphical password hotspot problem”, In 33rd Annual IEEE International Computer Software and Applications Conference, 2009.
[6] Weinshall D., “Cognitive Authentication Schemes Safe against Spyware”. In IEEE Symposium on Security and Privacy (S&P), 2006.