IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 6, Issue 2, February 2017

Improved Pass-Matrix for Graphical Authentication

Harsha Mathur[1], Vijay Lokhande[2]

BIST Bhopal[1, 2]

Abstract: Graphical authentication is widely used everywhere these days. Graphical authentication schemes are broadly categorized as recognition based, recall based and cued-recall techniques. All the techniques which comes under these categories are discussed in this paper. In this paper an improved pass matrix scheme is proposed and analysis is done by 50 random users and it is found that proposed scheme provides a secure and more convenient way of graphical authentication.

Keywords: Graphical Authentication, cued-recall techniques, proposed scheme, Déjà vu, Passfaces.

I. INTRODUCTION

The Internet connectivity has converted the whole world into a global village and at the same time created many security problems. For any organization, it is essential to protect its internal resources from security threats from all over the world. Security has three important goals - confidentiality, integrity and availability. Confidentiality refers to providing access to only authorized users, integrity refers to preventing from unauthorized changes and availability refers to providing access to authorized users at any time [54,81]. Confidentiality can be provided by authentication and encryption. Authentication is the first level of security for resources to prevent intruders and to provide access only to the legitimate users. It is difficult to compromise a system that has preventive measures. Intrusion is any activity that compromises the security of a system. The main aim of the intruder is to access the system resources pretending like a legitimate user either by guessing the passwords or by stealing the passwords. Graphical passwords can be categorized into three methods recognition based, recall based and cued recall based on the cognitive load on the user in retrieving the passwords from the memory. The metrics considered for memorability and usability are recall success rate, password registration (creation) time, login time and the errors made by the users while entering the password. The security is verified by the resistance against password guessing and the password capturing attacks. Brute force, dictionary and (personalized) guessing attacks are password guessing attacks. Shoulder surfing, social Engineering and malware attacks are password capturing attacks.

II. GRAPHICAL AUTHENTICATION TECHNIQUES

2.1 Recognition based techniques

In recognition based systems, users generally choose a set of pictures throughout password registration and he needs to acknowledge these pictures throughout login time. The studies of cognitive scientists say that humans have unlimited memory for photos and they will keep in mind and recall photos simply than text [9]. Hence, the precise recall of textual passwords is replaced by recognizing pictures to scale back the cognitive load on the user.

Deja Vu

Dhamija and perrig [13] designed a graphical system known as deja vu exploitation recognition primarily based authentication. In this technique, from a set of sample images, user selects a fixed variety of pictures to make a picture portfolio. During login time, a challenge set with number of pictures can be displayed on the user‟s system. The challenge set contains a few pictures from the user‟s portfolio and therefore the remainder of the pictures from the remaining image samples that are known as as decoy images. For authentication user must acknowledge the pictures from his portfolio that are a part of the challenge set. The pictures are random art pictures generated exploitation an initial seed and therefore the server maintains ten thousand seeds of random art pictures for choice of images by the user to make his portfolio.

Passfaces

Real User Corporation developed the technique Passfaces. Many researchers worked on finding the effect of pictures than text on human brain. They reported that humans are good in recognizing pictures or images than text. In this technique, user selects a set of human faces during password creation.

During login, a panel of human faces will be displayed in a grid in multiple rounds and the user must recognize the face that belongs to his portfolio in each round. The face should be correctly recognized in all rounds for authentication. For testing 3x3 grid is used with five rounds. The official website reported the password creation time as 3 to 5 minutes for a panel of 9 faces in 5 rounds. The password complexity is 9^5.

DOI 10.17148/IJARCCE.2017.6232

Faces / Story

Davis et al [9] proposed 2 authentication systems – Faces (based on Passfaces) and Story(based on order of images). In faces scheme, during password creation, user selects a set of faces, each face from a totally different category of faces. There were 12 categories of faces like typical Asian male and feminine, typical black male and female etc. In Story system, during password creation, user selects a sequence of pictures and makes a story with the images to recollect the sequence. The pictures for Story are taken from differing types of images like animals, children, sports, male and female models that are utilized in on a daily basis to day life. During login, user has to identify the pictures within the same sequence. Dumphy et al [10] tested the Passfaces authentication system against social engineering attack. They found that the success of the attack can be reduced by selecting decoy pictures rigorously. Tari et al [12] investigated for shoulder surfing attack on Passfaces. They showed that usage of mouse was more vulnerable than victimisation keyboard. In case of usage of keyboard, the intruder has to use key loggers and screen scrapers to capture the passwords.

For mobile devices

Jansen et al [11] designed a system for mobile devices such as PDAs. In this graphical authentication system, themes (like cat, sea etc.) are used wherever every theme contains thirty thumb nail photos. During registration, user selects a theme then selects a sequence of thumbnail photos on the theme. For authentication, during login time, user recognizes and touches the thumb nail photos elite by him in the same sequence using stylus. A number is appointed to every thumbnail icon and therefore the sequence of thumbnail photos kind variety password. One drawback of this technique is that since the quantity of thumbnail pictures is proscribed to thirty, the password house is little.

2.2 Recall based techniques

The (pure) recall based passwords are same as ancient passwords as they need the user to keep in mind and recall the passwords throughout login time. In recall based systems, users draw their password either on a blank canvas or on a grid. There are no cues to assist the user to recall the passwords. The cognitive load on the user is a lot of and it is tougher than all different techniques [8].

DAS (Draw-A-Secret)

Jermyn et al [7] proposed a graphical password technique that is a lot of secure than matter passwords. In this technique, user draws a secret (picture) on a grid using stylus throughout password registration. The password is an ordered sequence of coordinate pairs of grid cells touched throughout the password drawing by the user. The drawing may contain one or a lot of pen strokes separated by pen up events. For authentication, during login time, user has to draw the image touching the grid cells within the same sequence. Considering the dimensions of memorable graphical passwords with the size of the wordbook of usual matter passwords, DAS was claimed as more secure than ancient system.

Passdoodle

Passdoodle allows users to produce hand written drawings as passwords with a stylus on barely screen while not an obvious grid. Goldberg et al [6] conducted user study on a paper using Passdoodle and found that users were ready to keep in mind their passwords but unsuccessful in recalling the order or direction of the pen strokes. For password registration, the technique requires coaching to acknowledge the password. The success depends on the user‟s ability to recall and reproduce their doodles. This technique is susceptible to shoulder surfing, one login may be enough to look at the password. No further study was done on this technique.

Pass-Go

Tao and Adams [5] designed a new scheme Pass-go based on Chinese board game Go. User draws word on the grid using intersections of the grid cells. For each intersection, sensitive spaces are outlined and touching any purpose within a sensitive area is equal to touching the intersectant purpose. The grid of size (G+1) x (G+1) in DAS is equal to G x G grid in Pass-go. An ordered sequence of intersectant points with pen up events forms the word. Colors will be wont to produce robust passwords. They conducted user study and reported that Pass-go keeps most of the benefits of DAS theme and offers a lot of security and higher usability.

PassShapes

De Luca et al [4] evaluated totally different authentication techniques for ATM usage and found that several users rely on the shapes so as to recollect the PIN. In an on-line survey, 86 members participated and four-hundredth of them expressed that they use geometric shapes to bear in mind the word. A shape word could contain several shapes like sq. followed by rectangle. Instead of remembering the PIN, they remember the form on the key pad and enter the digits within the form as word

2.3 Cued-recall techniques

Cued-recall is an easier task than pure recall because cues help the users to recall the password. In cued-recall systems, generally users select specific locations on a single image. Instead of remembering the entire image, user has to remember few locations on the image.

- **PassPoints**

G.E. Blonder [3] designed the first graphical authentication technique. In this technique, user selects certain locations on an image as password. During login time, user has to reselect the same locations in the same order for authentication. No user study was done for this. Users can not click on the background in password selection as it was simple.

- **Cued click points**

Chiasson et al [2] proposed cued click points and persuasive cued click points. In Cued click points, user

DOI 10.17148/IJARCCE.2017.6232

clicks on one point on an image to go to next round. Another image will be displayed in that round and the user has to click a point in that image. This process will be repeated five times making a password of five click points for five images. During login user has to click the same points in the same sequence. If the user clicks a wrong point, an unknown image will be displayed which gives an implicit feed back to the user. Then, the user restarts the process. Implicit feedback is not useful in the case of intruder because he knows nothing about images.

- **S3PAS**

Zhao and Li [1] proposed a shoulder surfing resistant authentication system S3PAS. During registration user selects a password and the characters in the password are known as original pass characters. The login image of S3PAS consists of randomly scattered 94 printable characters. For authentication, user has to find the positions of original pass characters and assumes invisible triangles known as pass triangles for every three pass characters in sequence. The user has to click inside the pass triangle following some rules. The clicks in sequence generate a session password.

3. IMPROVED PASSMATRIX APPROACH FOR GRAPHICAL AUTHENTICATION

Figure shown below is the flowchart of the registration phase. At this stage, the user creates an account which contains a username and a password. The password consists of only one pass-square per image for a sequence of n images. The number of images (i.e., n) is decided by the user after considering the trade-off between security and usability of the system. The only purpose of the username is to give the user an imagination of having a personal account. The user can either choose images from a provided list or upload images from their device as pass-images. Then the user will pick a passsquare for each selected pass-image from the grid, which was divided by the image discretization module. The user repeats this step until the password is set.

Authentication phase

Figure shown below is the flowchart of the authentication phase. At this stage, the user uses his/her username, password. The following describes all the steps in detail:

1) The user inputs his/her username which was created in the registration phase.

2) A new indicator comprised of a letter and a number is created by the login indicator generator module. The indicator will be shown when the user uses his/her hand to form a circle and then touch the screen. In this case, the indicator is conveyed to the user by visual feedback.

3) Next, the first pass-image will be shown on the display, with a horizontal bar and a vertical bar on its top and left respectively. To respond to the challenge, the user flings or drags the bars to align the pre-selected pass-square of the image with the login indicator.

4) Repeat step 2 and step 3 for each pre-selected passimage.

5) The communication module gets user account information from the server through HttpRequest POST method.

6) Finally, for each image, the password verification module verifies the alignment between the passsquare and the login indicator. Only if all the alignments are correct in all images, the user is allowed to log into PassMatrix.

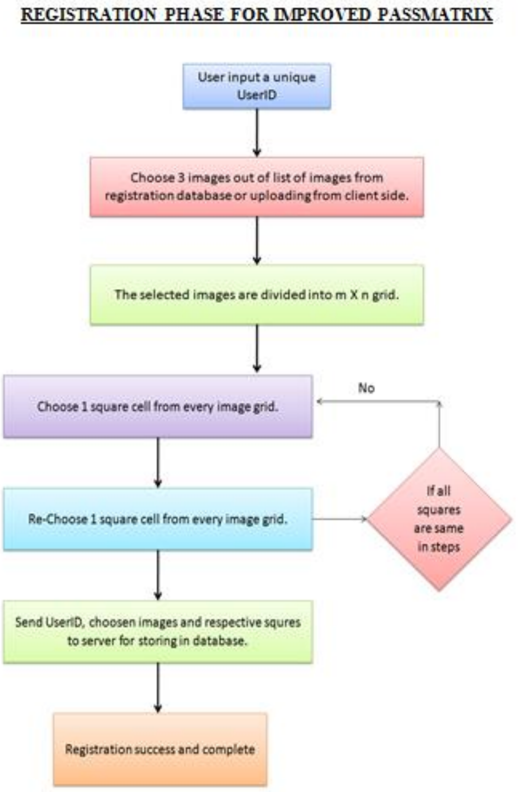
REGISTRATION PHASE FOR IMPROVED PASSMATRIX
User input a unique UserID
Choose 3 images out of list of images from registration database or uploading from client side.
The selected images are divided into m X n grid.
Choose 1 square cell from every image grid.
No
Re-Choose 1 square cell from every image grid.
If all squares are same in steps
Send UserID, choosen images and respective squres to server for storing in database.
Registration success and complete

Fig 1: Showing registration phase for improved passmatrix

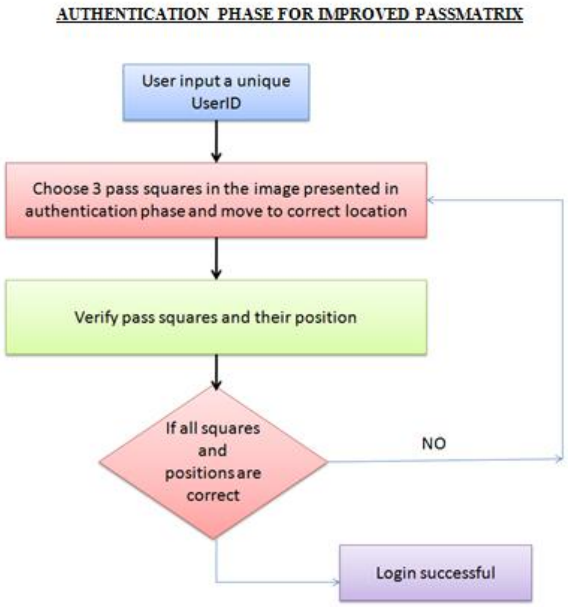
AUTHENTICATION PHASE FOR IMPROVED PASSMATRIX
User input a unique UserID
Choose 3 pass squares in the image presented in authentication phase and move to correct location
Verify pass squares and their position
If all squares and positions are correct
NO
Login successful

Fig 2: Authentication phase for passmatrix

DOI 10.17148/IJARCCE.2017.6232

Questions	Improved PassMatrix	PassMatrix
Some information is exposed when authenticating in public.	4.6	4.13
I would have serious loss if my passwords were cracked.	4.3	4
Compared to text passwords and PIN, improved PassMatrix is more secure.	4.58	4.27
PassMatrix is secure and trustable.	4.47	4.27
It's difficult to find out the pass-square of others even if I had screen shots or videos of one's login process.	4.9	4.27
It's easy and fast to create an account in Pass-Matrix.	3.7	3.87
In general, PassMatrix is a user-friendly system and is easy to use.	4.10	4.2
The time consumed for using PassMatrix is acceptable.	4.08	4.07
I tend to choose squares that are eye-catching.	4.2	3.83
I tend to choose squares that are obtrusive.	2.4	2.6

Tested by 50 users for guessing password of another user		
Success	All three pass squares and all respective position is found correct	0
Failure	1 pass square correct	5
	2 pass square correct	2
	3 pass square correct	0
	1 pass square correct with 1 position correct	3
	2 pass square correct with 1 position correct	0
	2 pass square correct with 2 position correct	0
	3 pass square correct with 1 position correct	0
	3 pass square correct with 2 position correct	0
	0 coorect	43

Accuracy of improved Pass-matrix scheme within 5 tries	
REGISTRATION PHASE	**97%**
AUTHENTICATION PHASE	**98%**

Time analysis for authentication phase for improved Pass-matrix			
	Mean	**Median**	**Standard deviation**
Time (in sec)	**116**	**97**	**37**

CONCLUSION

It is found that graphical password prove to be a more secure way of authentication and no scheme gives protection from all attacks yet they have different password spaces and probabilities to be cracked. Hybrid approaches prove to be a better option for authentication. In this paper an improved pass matrix scheme is proposed and results are compared with base approach. It is found that proposed approach outperforms better.

REFERENCES

[1] Zhao, H. and Li, V., "S3PAS: A Scalable Shoulder-Surfing Resistant Textual- Graphical Password Authentication Scheme," 21st International Conferenceon Advanced Information Networking and Applications Workshops (AINAW07), vol. 2. Canada, pp. 467-472, 2007

[2] Chiasson, S., Van Oorschot, P., and Biddle, R., Graphical password authentication using Cued Click Points. In European Symposium on Research in Computer security (ESORICS), LNCS 4734, pages 359/374, September 2007.

[3] Blonder, G., Graphical passwords. United States Patent 5,559,961, 1996.

[4] Alexander De Luca, Rom a Weiss, Heinrich Hussmann "PassShape – Stroke based Shape Passwords". In Proceedings of OzCHI 2007, 28-30 November 2007, Adelaide, Australia.

[5] Tao, H. and Adams. C., Pass-Go: A proposal to improve the usability of graphical passwords. International Journal of Network Security, 7(2):273{292}, 2008.

[6] Goldberg, J., Hagman, J., and Sazawal, V., Doodling our way to better authentication (student poster). In ACM Conference on Human Factors in Computing Systems (CHI), April 2002.

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

[8] Craik, F. and McDowd, J. Age differences in recall and recognition. Journal of Experimental Psychology: Learning, Memory, and Cognition 13, 3 (July),474–479. 1987.

[9] Davis, D., Monrose, F and Reiter, M., On user choice in graphical password schemes. In 13th USENIX Security Symposium, August 2004.

[10] Dunphy, P. Nicholson, J. and Olivier, P., Securing Passfaces for description. In 4th Symposium on Usable Privacy and Security (SOUPS), July 2008.

[11] Jansen. W., "Authenticating users on handheld devices".Proceedings of the Canadian Information Technology Security Symposium, 2003.

[12] Tari, F. Ozok, A. and Holden, S., A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In 2nd ACM Conference on Symposium on Usable Privacy and Security (SOUPS), July 2006.

[13] Dhamija, R., and Perrig, A., D_ej_a Vu: A user study using images for authentication. In 9th USENIX Security Symposium, 2000.

DOI 10.17148/IJARCCE.2017.6232