ISSN 2348 – 7968

A Comprehensive Survey on Graphical Passwords and shoulder surfing resistant technique analysis

J. Thirupathi

Associate Professor, Dept of Computer Science and Engineering.

Abstract: For any organization, it is essential to protect its all private resources from security threats from all over the world. The most general computer authentication method is to use alphanumerical usernames and passwords. Traditional alphanumerical passwords are vulnerable to many attacks. Graphical passwords are introduced as alternatives to textual passwords to overcome these problems. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is hard to remember. To solve this problem, some researchers have developed authentication methods that use pictures as passwords. The fact is that humans can remember pictures better than text. During password creation, the user selects a theme consisting of photos in thumbnail size and set a sequence of pictures as a password. During authentication, user must recognize the images in the correct order. Each thumb nail image is assigned a numerical value, thus the sequence of the chosen images will create a numerical password. In this paper, we conduct a comprehensive survey of the existing graphical password techniques. This paper publishes the analysis of graphical passwords and shoulder surfing resistant technique. Shoulder-surfing is a known risk where an attacker can capture a password by direct observation or by recording the authentication session.

Keywords: Graphical Passwords, Textual Password, Shoulder-surfing**.**

1. INTRODUCTION

The alphanumeric password has been part of the authentication process for a very long time. The most common computer authentication method is for a user to submit a user name and a text password. 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. However, this simple and ubiquitous technology has some well-known usability problems especially on the memorability aspect. The humans ability to remember pictures better than text has been well documented in numerous cognitive and psychological studies that are graphical passwords [1]. As a result, much research has been inspired in both the security and Human Computer Interaction communities in recent years to explore graphical authentication systems as an alternative or an enhancement to text passwords. As the name implies, graphical authentication uses graphics (pictures, icons, faces etc.) instead of the common used text strings.

Attacks on knowledge-based authentication can be categorized into password guessing attacks and password capturing attacks. The password guessing attacks may be online attacks or offline attacks. For offline attacks, for checking every possible combination, server side password file should be captured by the intruder which is a difficult task. In password guessing attacks, attackers exhaustively search through the entire theoretical password space, or predict more likely passwords using a dictionary or personal information of the user to obtain an acceptable success rate within a manageable number of guesses. It is not possible to verify all combinations in online attacks because after a limited number of unsuccessful logins, the system blocks the user.

Graphical passwords are still far from being perfect. For example, a password supplied for authentication by a user in a public place, if not properly protected, can be stolen by a bystander who observes over the user’s shoulder. This is known as a shoulder surfing attack and commonly regarded as a drawback to various graphical password systems. Alpha-numeric passwords are defended against this by substituting asterisks for the password characters in the display as the user logs in. To make graphical passwords reliable in the real world, it is essential to arm them with good shoulder surfing defence mechanisms.

Many researchers worked on authentication systems and designed various graphical password techniques to enhance the usability and security. No author has measured all the metrics of usability and security, only some of the aspects are highlighted by each author. For some proposed techniques, no user study was done. There is no standard defined for measuring these metrics and each author followed their own methods to evaluate memorability, usability and security. So it is not possible to compare the results of various methods and make conclusions. We discuss the method followed by the author and the results reported by him as part of evaluation.

In this paper, we study shoulder surfing defences for recall-based graphical password systems such as Draw-A-Secret (DAS), Background Draw-A-Secret (BDAS) and Pass-Go. DAS is a representative graphical password scheme and worthy of extensive study for the following reasons. First, its theoretical password space can be larger than that of text passwords. Second, unlike many other graphical password systems, DAS can be used for not only user authentication, but also for key generation. Although some research has revealed that the user choices of DAS passwords could render this theoretically sound scheme less secure in practice, it appears that many of the weaknesses could be improved by introducing a background image into the drawing grid, together with other countermeasures.

Drawing the password in Pass-go is difficult than DAS, and remembering the sequence of dots or lines is some hard task.

2. Overview of Authentication Scheme

Current authentication methods can be divided into three main areas:

1. Token based authentication
2. Biometric based authentication
3. Knowledge based authentication

Token based techniques, such as key cards, bank cards and smart cards are widely used. Each character may contain one or more strokes. A stroke is an ordered list of cells. A password is represented by a sequence of strokes. The length of a stroke is the number of cells it contains. The length of the password is the sum of the lengths of its strokes. Many token-based authentication systems also use knowledge based techniques to enhance security.

Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security.

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage.

Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

Graphical passwords were introduced as alternatives to textual passwords where in user visualizes a picture or multiple pictures to create a password. Many psychology studies have shown that the humans have superior memory for recognizing and recalling visual information opposed to verbal or textual information. The attack programs should automatically generate accurate mouse movements to imitate human input, which is a difficult task.

Graphical passwords can be divided into three categories– recognition based, recall based and cued recall techniques. The recognition based, recall based and cued recall techniques are occasionally referred to as cognometric, draw metric and loci metric system respectively. Many techniques have been proposed in these three areas to overcome the difficulties of textual passwords. For graphical authentication technique, important issues are number of rounds required for authentication, number of pictures that should be displayed on the screen, number of images to be selected in each round and order/unordered selection of pictures.

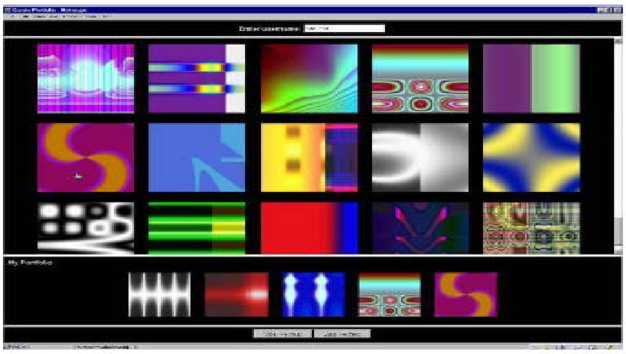
3. Survey on Graphical Passwords

The three types of techniques - recognition based, recall based and cued recall. Techniques are given bellow.

3.1 Recognition Based Techniques

a) Déjà vu [2] In this recognition based systems, users generally select a set of images during password registration and he has to recognize these images during login time. The studies of cognitive scientists say that humans have unlimited memory for pictures and they can remember and recall pictures easily than text. Hence, the precise recall of textual passwords is replaced by recognizing images to reduce the cognitive load on the user.

Deja Vu using recognition based authentication. In this technique, from a set of sample images, user selects a fixed number of images to form an image portfolio. During login time, a challenge set with number of images will be displayed on the user's system. The challenge set contains a few images from the user's portfolio and the rest of the images from the remaining image samples which are called as decoy images. For authentication user must recognize the images from his portfolio which are part of the challenge set. The images are random art images generated using an initial seed and the server maintains 10000 seeds of random art images for selection of images by the user to form his portfolio.



Portfolio selection window for Deja Vu

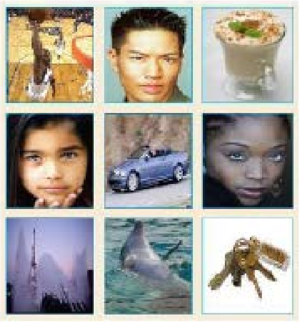
b) Passfaces

Real User Corporation developed the technique Passfaces[3][4]. 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}

c) Faces / Story

Davis et al [5] proposed two 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 different class of faces. There were 12 classes of faces like typical Asian male and female, typical black male and female etc. In Story system, during password creation, user selects a sequence of images and makes a story with the images to remember the sequence. The images for Story are taken from different types of images like animals, children, sports, male and female models which are used in a day to day life. During login, user has to identify the images in the same sequence.



Sample panel for Story

They conducted user study of these two techniques and found that story passwords were difficult than Face passwords. Nearly half of the participants didn't form a story, they just selected four interesting pictures and tried to remember the sequence of selection. But recalling the images in sequence is a difficult job unless the selected images are linked by some concept.

In recognition based systems, users select a set of images or faces forming a portfolio from a large database during password registration and he has to recognize the images Introduction 9 or faces from his portfolio in a challenge set during login time. A number of researchers studied the effect of pictures and objects in learning and recalling by humans. The recognition based technique is the easier task than the recall based technique

d) For mobile devices

Jansen et al. [6] proposed a graphical password mechanism for mobile devices. During the enrolment stage, a user selects a theme which consists of thumbnail photos and then registers a sequence of images as a password or numbers. During the authentication, the user must enter the registered images in the correct sequence. One drawback of this technique is that since the number of thumbnail images is limited to 30, the password space is small.Each thumbnail image is assigned a numerical value, and the sequence of selection will generate a numerical password. The result showed that the image sequence length was generally shorter than the textural password length. To address this problem, two pictures can be combined to compose a new alphabet element, thus expanding the image alphabet size.

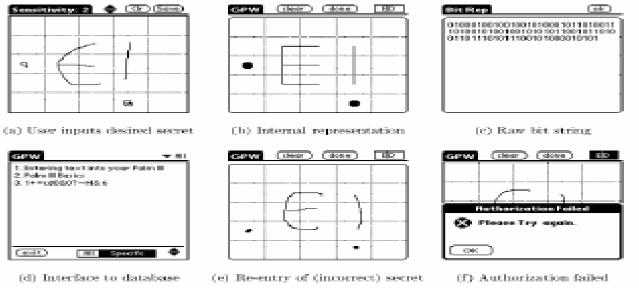
User selected theme for a mobile

3.2 Recall based techniques

The recall based passwords[7] are same as traditional passwords as they require the user to remember and recall the passwords during login time. In recall based
systems, users draw their password either on a blank canvas or on a grid. There are no cues to help the user to recall the passwords. The cognitive load on the user is more and it is harder than all other techniques

a)DAS (Draw-A-Secret)

Jermyn [8] proposed a graphical password technique which is more secure than textual passwords. In this technique, user draws a secret (picture) on a grid using stylus during password registration. The password is an ordered sequence of coordinate pairs of grid cells touched during the password drawing by the user. The drawing may contain one or more pen strokes separated by pen up events. For authentication, during login time, user has to draw the picture touching the grid cells in the same sequence. Considering the size of memorable graphical passwords with the size of the dictionary of usual textual passwords, DAS was claimed as more secure than traditional system.



(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

A DAS password

Nali and Thorpe [9, 10] conducted a user study on paper. Users were requested to draw the passwords on a paper to measure the predictable features in passwords selected by the users. They reported some symmetry and no predictions about start and end points of strokes. They showed that 45% of the passwords were symmetric, 80% of the passwords contain 1-3 strokes and 86% were centred or approximately centred within the grid. According to their report, 29% of the passwords drawn were invalid because users draw the strokes too close to a grid line.

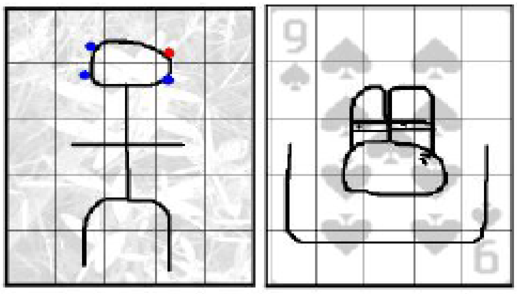
b)Background DAS (BDAS) (cute recall) In 2007, this method proposed by adding background image to the original DAS for improvement, so that both background image and the drawing grid can be used to providing cued recall [11]. The user starts by using three different ways:

i. The user have secret in mind to begin, and then draw using the point from a background image.

ii. The user's choice of secret is affected by various characteristic of the image.

iii. A mix of two above methods.

Bellow Figure shows a sample of BDAS algorithm.

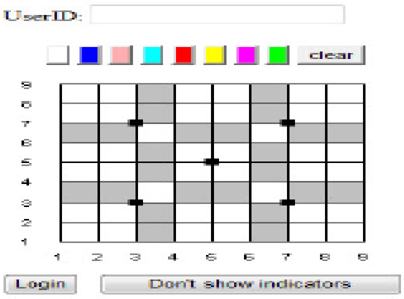


(a) (b)

With reference to a research on BDAS, memory decaying over a week is one of the major problems in this algorithm. Users had no problem in recreating it in the five-minute test, but a week later they could not do better than producing the secret password as previous. Also shoulder-surfing and interference between multiple passwords are concerns for BDAS

c) Pass-Go

Tao and Adams[12] designed a new scheme Pass-go based on Chinese board game Go. User draws password on the grid using intersections of the grid cells. For each intersection, sensitive areas are defined and touching any point inside a sensitive area is equal to touching the intersecting point. The grid of size (G+1)x(G+1) in DAS is equal to GxG grid in Pass-go. An ordered sequence of intersecting points with pen up events forms the password. Colors can be used to create strong passwords. They conducted user study and reported that Pass-go keeps most of the advantages of DAS scheme and offers more security and better usability. In Pass-go, dot and line indicators are used to display the password. By using an encoding scheme, the password can be inputted using keyboard. They conducted user study with 158 participants over a period of three months.



Login screen for Pass-Go

They reported the success rate as 78% and the weekly success rate varied from 68% to 95%. Pass-go has more password space than DAS. For a password of length n, for pass-go-9 the password space is 77 bits.

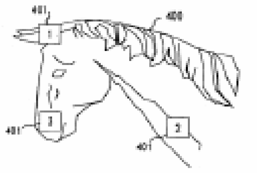
Drawing the password in Pass-go is difficult than DAS, and remembering the sequence of dots or lines is also a difficult job. It may not be convenient to draw some shapes using only intersecting points or lines. Por et al [13] added background images to Pass-Go to support the user in remembering the password. This technique is more vulnerable to shoulder surfing.

3.3 Cued-recall techniques

Cued-recall is an easier task than pure recall because cues help the users to recall the password [14]. 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.

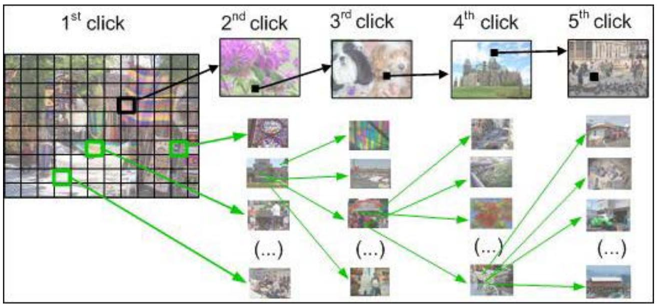
a)Pass Points

G.E. Blonder [15] 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.



b)Cued click points

Chiasson et al[16] proposed cued click points and persuasive cued click points. In Cued click points, user 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



Cued click points

. Implicit feedback is not useful in the case of intruder because he knows nothing about images They conducted user study and reported password registration time as 25 seconds, login time as 7 seconds and login success rate as 96%. They analyzed the user choice in click points and found that passwords are predictable because most of the click points fall within known hotspots. Chiasson et al [17] proposed persuasion to influence user choice in click-based graphical passwords, encouraging users to select more random, and hence more difficult to guess, click-points. Persuasive technology motivates and influence people to behave in a desired manner.

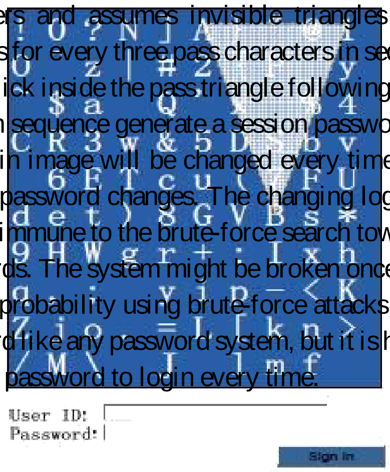
4 Shoulder surfing resistant techniques

Graphical passwords are more vulnerable to shoulder surfing attacks than conventional textual passwords; research has been done to study the difficulty of cracking graphical passwords. Because graphical passwords are not widely used in practice, there is no report on real cases of breaking graphical passwords. Here we briefly exam some of the possible techniques for breaking graphical passwords and try to do a comparison with text-based passwords. The intruder captures the password either by direct observation or by using hidden cameras. Many shoulder surfing resistant techniques have been proposed and each technique has its own way in providing security against shoulder surfing attack.

S3PAS

Zhao and Li [18] 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.

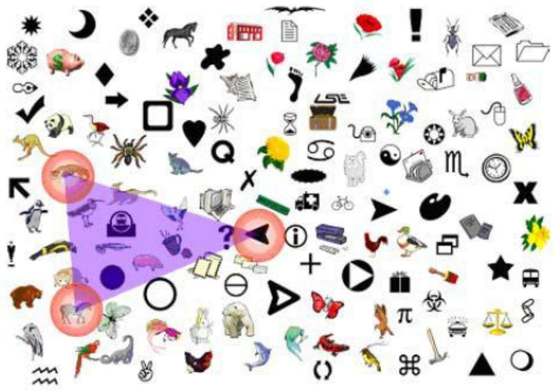
The login image will be changed every time and in turn the session password changes. The changing login image makes S3PAS immune to the brute-force search towards the session passwords. The system might be broken once by chance with a small probability using brute-force attacks towards session password like any password system, but it is hard to get actual original password to login every time.



Graphical interface for S3PAS

Convex Hull click

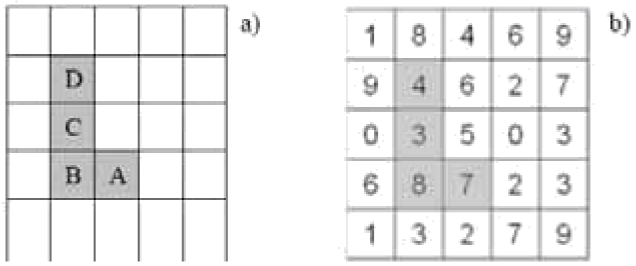
Sobrado and birget [19] developed shoulder surfing resistant graphical authentication technique. During registration, user selects pass objects from a set of objects. The login involves several rounds. For authentication, user recognizes pass objects and clicks within the convex hull of 3 pass objects. It is impossible to clearly identify pass objects on the login interface if 1000 objects are used as specified by the authors. The login time with 5 challenge was 72 seconds. The time required to rearrange the icons between the challenges was 17 seconds and total login time was 89 seconds.



Graphical interface for Convex Hull Click

GrIDsure

GrIDsure[23,21] is a pattern based authentication. Humans remember patterns much better than PINs, and this helps to



a)

	D			
	C			
	B	A		

b)

1	8	4	6	9
9	4	6	2	7
0	3	5	0	3
6	8	7	2	3
1	3	2	7	9

create session PINs using dynamic grid. They enter PIN based on the pattern selected by him during registration. During login, a grid is displayed with randomly placed digits. User follows his pattern and enters the digits in pattern as PIN. For the pattern in the fig 2.17, the PIN is 7834. This technique is strong against shoulder surfing when the intruder captures password only. If the intruder captures both login grid and the password, it is easy to get the password.

A pattern for GrIDsure

Weber analyzed and reported that GrIDsure Passwords are much more secure than traditional PINs against shoulder surfing attacks. Bond[15] analyzed GrIDsure and reported weaknesses of the technique.

Shoulder surfing defence

Zakaria et al [20] proposed shoulder surfing defence for recall based graphical passwords. They proposed three techniques for protecting DAS systems from shoulder surfing – decoy strokes, disappearing strokes and line snaking. Decoy strokes draw additional strokes in addition to the strokes drawn by user while drawing the secret. Disappearing stroke defence scheme removes the stroke from the screen after it was drawn by the user. Line snaking scheme disappears the stroke drawn by the user, but it leaves some portion of it on the screen for some time. They evaluated the security and usability of the techniques and reported that 63% of the passwords were stolen in DAS and 57% passwords stolen using decoy strokes. Disappearing strokes scheme and line snaking capture 20% of the passwords. These schemes are vulnerable to hidden cameras and malware attacks.

5 Analyses

Recognition based techniques are good in memorability; users are able to remember and recognize the passwords successfully. The server has to maintain large number of images or faces and for every round of authentication; server has to prepare the challenge set for every user. Due to the limited number of images in the challenge set and few rounds used for authentication, the password space is less in recognition based techniques and in turn these are vulnerable to password guessing attacks. The Password capturing attacks require multiple logins to get the complete portfolio of the user. The password creation time and login times are more compared to recall based techniques.

Recall based techniques have large password space and are secure against password guessing attacks. There is no need to maintain large number of images or faces by the server and no requirement of forming the challenge set. The Password creation and login times are less than the other two techniques. The recall based techniques are vulnerable to password capturing attacks because in a single session or by single observation the intruder may get the password. The password complexity depends on the number and the length of the strokes in password. But it is difficult to remember the order of the multiple strokes in random shape passwords. Drawing a password with mouse is inconvenient.

Cued recall systems are good in memorability. Cues help the users to retrieve the passwords from memory without writing anywhere. The security of passwords in cued recall system depends on the image selected for authentication. Generally, images will be having limited number of clickable points for password selection which reduces the password space and in turn, passwords are vulnerable to password guessing attacks. These are vulnerable to password capturing attacks because entire password or user's portfolio will be displayed for every login which can be observed by the intruders. Password creation and login times are more compared to recall systems. The details collected for various graphical authentication techniques from different sources (approximate values) and shoulder surfing systems were given in bellow tables. Each technique has its own way for evaluation of usability and security.

Name	Register time	Login time	Type	Recall rate
Deja Vu	40-50	25-32	Recogn	88-100%
Passfaces	150-250	15-75	Recogn	75-100%
Faces/ Story	35-44	20	Recogn	80-85%
DAS			Recall	50-85%
BDAS			Recall	40-80%
PASS-GO			Recall	80%
PassPoint	55-90	10-20	Cued	50-92%
CCP	10-30	5-10	Cued	98%

Graphical authentication techniques

Name	Register time	Login time	Recall rate	Shoulder Surfing Rate
CHC		80	90%	
S3PASS			79%	
GrIDsure			85%	
DAS- Defence				20%
DAS-DS				55%

Shoulder surfing resistant systems

6 Conclusion

In this paper, we have conducted a comprehensive survey of existing graphical password techniques. The existing recognition based, recall based and cued recall techniques were discussed and analyzed. This paper also presents various existing shoulder surfing resistant techniques and analyzed. The current graphical password techniques can be classified into three categories: recognition-based ,recall-based and cued recall techniques. A comparison of current graphical password techniques is presented in Table 1and 2. Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument. Our preliminary analysis suggests that it is more difficult to break graphical passwords using the different traditional attack methods.

More research and user studies are required for graphical password techniques to achieve higher levels of maturity and usefulness.

7 References

[1]Monrose, F. and Reiter, M. Graphical passwords. *Security and Usability:Designing Secure Systems That People Can Use*, L. Cranor and S. Garfinkel, Eds. O"Reilly Media, Chapter 9, 157–174. 2005.

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

[3]Passfaces Corporation. The science behind Passfaces. White paper, http://www.passfaces.com/enterprise/ resources/ white papers.htm.

[4] Real User Corporation: Passfaces. http://www.passfaces .com.

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

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

[7] 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

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

[9]Nali, D., Thorpe, J., Analyzing user choice in graphical passwords. Technicalreport, TR-04-01, School of Computer Science, Carleton University, May 2004.

[10]Thorpe, J. and Oorschot, P. C. V., Graphical dictionaries and the memorable space of graphical passwords. *Proceedings of the 13th USENIX Security Symposium*, San Deigo, CA, 2004.

[11] Chiasson, S., Forget, A., Biddle, R., and van Oorschot, P. 2008. Influencing users towards better passwords: Persuasive Cued Click-Points. In *Human Computer Interaction (HCI), The British Computer Society*.

[12] 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.

[13] Por, L. Y., Lim, X. T., Su, M. T., and Kianoush, F., The design and implementation of background Pass-Go scheme towards security threats.*WSEAS Transactions on Information Science and Applications 5,* 6 (June), 943–952. 2008.

[14] Tulving, E. and Pearlstone, Z. Availability versus accessibility of information in memory for words. *Journal of Verbal Learning and Verbal Behavior 5,* 381–391. 1966.

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

[16] 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.

[17] Chiasson, S., Forget, A., Biddle, R., and van Oorschot, P. 2008. Influencing users towards better passwords: Persuasive Cued Click-Points. In *Human Computer Interaction (HCI), The British Computer Society*.

[18] Zhao, H. and Li, V., "S3PAS: A Scalable Shoulder-Surfing Resistant Textual- Graphical Password Authentication Scheme," 21st *International Conference on Advanced Information Networking and Applications Workshops (AINAW 07)*, vol. 2. Canada, pp. 467-472, 2007

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

[20] Zakaria, N.H., Griffiths, D., Brostoff, S., Yan, J. " Shoulder Surfing Defence for Recall-based Graphical Passwords " Symposium on Usable Privacy and Security (SOUPS) 2011, July 20-22, 2011, Pittsburgh, PA, USA.

[21] Sreelatha Malempati User Authentication Using NativeLanguage Passwords International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011

[22] Sreelatha Malempati, Shashi Mogalla, "A Well Known Tool Based Graphical Authentication Technique", in proceedings of the conference CCSEA 2011, CS & IT 02, pp. 97-104, DOI: 10.5121/csit.2011.1211

[23] GrIDsure Limited. http://www.gridsure.com.

Thirupathi Jangapally, (PhD) Post graduated in Computer science and engineering M.Tech from JNTUH and Graduated in CSE B.Tech from JNTU TS, INDIA. Have 9 years of teaching

experience, presently working as an Associate Professor in Department of Computer Science and Engineering. Research interests include Image processing, Data mining, Cloud computing and Information Security.