ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

A Survey on Graphical Password Authentication System and their Security Issues

Rebeiro Caroline Leontia Carlton Christopher[1], Huda Noordean [2]

P.G. Student, Department of Computer Science & Engineering, College of Engineering & Management, Punnapra, Kerala, India[1]

Assistant Professor, Department of Computer Science & Engineering, College of Engineering & Management, Punnapra, Kerala, India[2]

ABSTRACT: In these recent times, the most prominent user authentication method which is widely used is the traditional method, it includes "username" and "password". Thus, authentication in this method, is generally through text. This method has certainly shown drawbacks which cannot be neglected. For example, users choose simple and feasible passwords which provides hackers to crack them quiet easily. However, Strong passwords are difficult to remember thus users tend to write them down or try to save them on as files on digital device. Graphical password can be used as alternative to solve the issues related to the text-based authentication based on the fact that humans can tend to remember pictures better than text. Nowadays, many computer systems, networks and internet-based environment are trying to use of graphical authentication technique. Thus, foundation of an authentication system is to promote users to choose better password, which consequently increases security, usability and also improving the password space. In this paper, we accomplish a comprehensive survey of the existing graphical password schemes into recognition based, pure-recall based, cued-recall based and multifactor(hybrid) methods. We also present a review on strength and drawback of graphical password schemes. This paper also provides an analysis on the security features of graphical password scheme. In this paper, we have clarified problems, provided solutions and future work.

KEYWORDS: Graphical password, Authentication methods, Security attacks, Text passwords.

I. INTRODUCTION

Many passwords used are either weak-and-memorable otherwise difficult-to-remember, provided the fact that there is an immediate need for a secure and memorable password. Thus, the term authentication refers to the process that permits one entity to verify the identity of another entity . Information security is guaranteed by authentication. The method that is used to provide information security is use of passwords for authentication. There have been different schemes developed to provide security during authentication. Authentication schemes range from simple to complex. The most prominent form of authentication is with a username and password. The main problem with this, is difficulty to remember the password. Studies have shown that users often choose short passwords or passwords that are easy to remember [1]. Normal passwords can be easily hacked, stolen or forgotten [2]. In the recent computer world new article, security team of a large company executed a network password cracker and within a time period of 30 seconds they were able to identify 80% of the passwords [3]. Studies show that users have the tendency to write them down the password or use the same password for multiple accounts [4,5]. There are unlimited ranges on how a user can authenticate to any web application. Authentication schemes depends on the following three factors [6]:

1.Knowledge: what a user knows about the system. e.g.: password or security question

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

2.Possession: what a user has with himself about the system.eg: token or mobile phone.

3.Attribute: what a user is to a system. biometric characteristics like fingerprint, eye features etc...

Graphical Passwords have been used as an alternative method to the text-based schemes. Psychological studies have shown that humans are able to remember more visual information i.e. images better than text. [7]. In addition, the password space of a graphical password scheme increases as the number of picture is large thereby exceeding that of the text based scheme and thus offers better resistance to dictionary attacks. Due to these advantages, there has been a rapid and growing interest in graphical password. Graphical passwords have been applied to various applications such as ATM machines and mobile devices.

In this paper, we conduct a survey on the existing graphical password technique. We will discuss the strength and weakness of the graphical password schemes and also focus on the future scope in this field. In this survey, we want to answer to answer some questions such as:

1)Is graphical password more secure than text password?

2)What are the general issues in terms with design and implementation the graphical passwords?

3)What are the current weakness of each graphical password techniques?

This paper will be applied for researchers who are looking forward to develop a new graphical password technique and also industry practitioners who want to launch a better graphical password technique.

II. RELATED WORK

Graphical password is a type of knowledge based authentication. Thus, graphical passwords consist of images and visual representation which are used in replacement to text or alphanumeric characters.
The graphical passwords consist of four sections namely:
A) Recognition based technique
B) Pure Recall based technique
C)Cued-recall based technique
D)Hybrid based technique
a) Recognition Based Technique: In this technique, users have to choose the image or symbols from a set of images. At the time of registration, the users select images which is set as user's password. Thus, during authentication users have to remember this password from a collection of different images [8].90% of users were able to identify their password images. Also, users were able to remember their passwords after a time span of 45 days[9].

b) Pure recall based technique: In this technique users set as image as a password during registration. users need to reproduce or remember their own passwords and thus no clues are given to remind the passwords. This scheme is simple, easy but the difficulty in this technique is that passwords are hard to remember. It is more secure compared to recognition based scheme. It is quite similar to DAS (1999) and Qualitative DAS (2007).

c)Cued recall based technique: In this technique users generate a password during authentication with the help of a hints or reminders. It is quite similar to recall based scheme but it is recall with cueing.

d)Hybrid Based technique: In this technique authentication happens through the combination of two or more schemes. Thus, it overcomes the drawback of a single scheme. For e.g.: spyware, shoulder surfing etc...

A. Recognition Based Technique

In this technique users set as image as a password during registration. users need to reproduce or remember their own passwords and thus no clues are given to remind the passwords. This scheme is simple, easy but the difficulty in this technique is that passwords are hard to remember.It is more secure compared to recognition based scheme.It is quite

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

similar to DAS (1999) and Qualitative DAS (2007) recognition based scheme is also known as cognometric scheme or search scheme[10].

a) **Dhamija and Perrig [**4] proposed a scheme in the year 2000. In this scheme, users have to choose a random image from a set of images. The set of images are generated by the program executed in a system. During the authentication phase, the system provides the user with a set of images which consist of both decoy as well as password images. The user has to select the right set of images from a set of password and decoy images. The initial seeds are used to generate these images thus it becomes to store up but it is difficult to share or record these images. Deja vu scheme has its shortcomings such as ambiguous images are difficult to remember and the password space is less as compared to the textual password.

b) **Passface scheme** [11] was proposed by Brostoff.In this scheme, users have to choose four faces as a password. So, during the authentication phase, user is provided with a grid of size 3x3 shown in Fig 1, the user has to recognize one face from a set of nine face and click on it. This process continues until four faces have been selected by the user as a valid password. There are limitations such that it can be easily guessed and processing time is quiet longer than that of textual passwords.

c) **Jensen** [12] proposed a scheme in the year 2003.This scheme was mainly focused on PDAs. It is also known as **picture password scheme.** The user has to select image of size 40x40 from a 5x5 matrix. Thus, order of selection of image is also verified during the authentication phase i.e. It should be the same sequence of order as in registration phase. The disadvantage of this method is the memorability is more complex and difficult.

d) **Story** is quite similar passfaces scheme was proposed by Davis [13]. In this scheme, users have to select a sequence of images to form a portfolio. During login, users have to choose the images and their portfolio images. It is also required for the user to choose the image in the correct order to remember their passwords, user mentally construct a story by connecting the set of images.

e) **Sobardo and Birget** [14]proposed a scheme which focuses mainly on the shoulder surfing problem.In first method, the system displays a number of objects. During the authentication user chooses these pass-objects and click inside of a convex hull formed by the pass-objects.In order to show the password is difficult to guess. Sobardo and Birget formed a scheme, in which 1000 objects are used to make the display crowded and making it indistinguishable.

f) **Man et al** [15] proposed a method which is resistant to shoulder surfing attack. In Fig 2,The users have to select a number of images as a password object or pass-objects. Each pass-object has variants and each variant is assigned a unique code. Thus, during authentication user has to choose the pass-object from several scenes. Thus, user has to type a unique code along with a string along with a code indicating the relative location of the pass-objects.

Fig 1:Passface Scheme

Fig 2:Man et al Scheme

Cognitive authentication is an authentication mechanism used to restrict shoulder surfing attack and spyware. The user has to stand on the image of the portfolio and moves up, down, left or right edge, the column or row information is stored and along with this, a multiple-choice question is also included which gives the correct label of the path i.e. displayed in each round. Cognitive authentication calculates the cumulative probability and ensures that it was not entered just by chance after each round. The authentication is successful when it is above a threshold value.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

Graphical Password with Icons[GPI] [16] was designed to solve the problem of hotspot. In GPI users have to select 6 icons from 150 icons to set as a password. In this scheme, the GPIs system generate a password which is authenticated by the user and if the user is not satisfied with the password, the user can request to generate a new password. The drawback of this scheme is the icon size is very small and unacceptable login time.

B. Pure Recall Based Technique

Pure recall based scheme is also known as drawmetric scheme, where the users have to recall drawing on grid, that they selected registration phase. In this scheme, users have to draw password either onto a grid or a blank canvas.

a) **Jermyn** [17] proposed a method called "Draw-A -Secret"(DAS). Users have to draw a password on a 2D grid using stylus or mouse. The drawing may consist of a single stroke or multiple strokes. Thus, for the user to successfully login, users redraw the same path, passing through the grid cells as shown in Fig 3. The system database stores the password in the same sequence of coordinate of the grid encoded during the DAS password. The length of the password depends on the number of coordinate pairs. There is no need for user to remember any alphanumeric characters. The difficulty with this technique the user has to redraw at the exact position of the grid line.

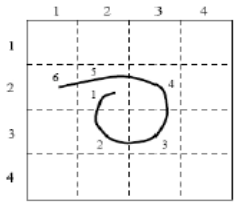

Fig 3:DAS Scheme

Fig 4:Passdoodle

b) **Thorpe and Van Oorschot** [18] proposed a graphical password scheme based on Jermyn. They introduced graphical dictionaries and using these dictionaries, they studied the brute force attack. They set a length parameter for DAS password and proved that DAS password of length 8 is less susceptible to dictionary attack. They also proved that space of mirror symmetric graphical password is smaller than DAS password space. People tend to recall symmetric images better than asymmetric images. Therefore, users tend to choose mirror symmetric passwords.

c) **Varenhorst** [19] proposed a graphical password scheme called **passdoodle** which allows user to create a free hand drawing as a password as shown in Fig 4. There is no visible grid. It consists of two pen strokes which drawn on the screen using a number of colors. Matching of passdoodle is more complex. In this system, doodle is stretched and scaled and then compared with stored user password.

d) **Weiss** [20] proposed the graphical password scheme **passhapes.** In the system, geometric shapes are generated on basis of the combination of eight strokes. During login, there is no grid and password can be drawn on any position. Thus, passshapes offer memorability.

e) **Syukri** algorithm [21]is based on pure recall based system, thus user is authenticated by drawing their signature with the help of a mouse or stylus. This method has two stages registration & verification. During registration, the user draws the signature with a mouse and system extracts area under signature and saves the information to the database. The verification stage involves the user to place signature and then extracts the parameter of the signature. Thus, verification involves using a geometric average and thus update a database. The biggest advantage there is no need to memorize one's signature and also signature are hard to fake.

There are two commercial products based on pure recall based graphical password scheme. First, there is an unlock scheme which is similar to a mini pass-go that unlocks screen of an android smart phones. In this user

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

chooses his unlocking pattern by dragging with finger over points in 3x3 grid. Second, in Windows 8 system, Microsoft has introduced a new graphical password. Users are provided with an image and have to draw gestures on the image provided. Gestures could include: top, circle and straight line or combination of these gestures.

Thus, these two products show that simple to operate easy to remember and can be applied to a system where there is no need for a high security level

C.Cued Recall Based Technique

Cued recall based scheme also known as Locimetric system is used to identify specific location. The user can recognize an image and choose arbitrary points on the image presented as password. The user has to click on the right points and also in the correct order of sequence of the image.

a) **Blonder:** This method was developed by Greg.E. Blonder [22] in which database consist of predefined images which will be displayed to the user has to tap region of interest as to set the password. The drawback to scheme region of selection is small and can be cracked. Blonder is the first technique used as graphical password, because of such limitations, this method was extended to a Draw-A-Secret.

b) **Passpoint:** It was designed to overcome the limitation of blonder [23]. The picture used is a password can be any natural picture provided that it should be rich enough to have many clicks points as shown in Fig 5. The image is not a secret and the user need not remember the click point of the image. Another flexibility point is that there are no predefined click regions like blonder algorithm. The user chooses several points in a particular order.

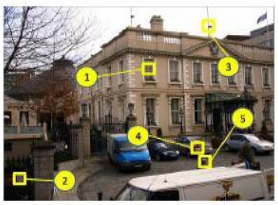

Fig 5:Passpoint

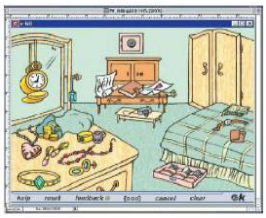

Fig 6:Passmap

a) **BDAS:** In 2007, this method proposes, background image and drawing grid used to provide cued recall. the users have three ways: users have a secret and then draw based on that using the point from background image. The user's choice depends on various characteristics of image. It consists of mix both methods

b) **PASSMAP:** The main problem is that good passwords are hard to remember password are simple to be cracked. Studies show that human memory are able to remember landmarks on a journey i.e. easy to remember. The passmap method is as shown in Fig 6.

c) **Passlogix Inc** is a security company in New York city [24]. This method repeats sequence of action, it means create a password by chronological situation. User selects the image based on the environment. For e.g. bathroom, bedroom enter the password as click or drag on items within image

d) **Cued click points** was proposed by chiasson [25]. In this method based on the location of the click point of the current image, the next image is displayed . Thus, the current image displayed is the function of coordinate of click points of previous image. If the user clicks on the incorrect point, the next image will be wrong one. however, most of times users tend to choose hotspot

e) **Persuasive cued click points** were proposed by chiasson [26]. This method includes persuasive feature to cued click point. Previous studies have showed that the security of click based graphical was reduce due to hotspots and patterns. Also, there arises an issue such that different users are attracted to the same spot of an image thus it makes the password predicable. To avoid such problem guidance is provided to prevent hotspots. Thus, by

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

adding a persuasive feature, it becomes less predictable and difficult to select password. The viewpoint is slight positioned to avoid hotspots. The viewport provides distinct points. Users can select within the viewport and not outside the viewport. A shuffle button is used to change the position of the viewport. The viewport and shuffle button are used during the password creation. Theoretical password spaces means total number of passwords that could be produced by the system for PCCP .

D.HYBRID BASED TECHNIQUE

Hybrid schemes is generally a fusion of two or more graphical password schemes. The hybrid scheme was used to overcome limitations of a single scheme such as spyware, shoulder surfing etc.

a) **Jiminy** [9] proposed a scheme in which user are provided an image as a reminder to choose graphical passwords that are easy to remember. In this scheme, templates based on a color combination are provided to the user which contains of holes. Initially, user selects an image along with a color template and have to click on the specific location within the image and then choose the position to place the template and store the password. During login, user choose the template and place them in specified location and then enters character which is visible from the holes. Users can remember the password as it requires only to identify the correct location of the image.

b) **Gao** proposed a scheme [27] which uses **CAPTCHA (**Completed Automated Public training Turing tests to tell Computer and Humans Apart). Thus, it provides features of both Graphical Password scheme as well as CAPTCHA technology. During registration, user selects the image as their password.at the time of authentication, user choose the password image from decoy of images and types the password CAPTCHA below every password image.

c) **Zhao and Li** [28] proposed a textual password graphical password authentication scheme**(S3PAS)** which combines features of both textual as well as graphical passwords and it is resistant to attacks such as spyware, shoulder surfing etc... During registration, users have to choose string K as a text password. During login, users has to find the original password from a login image and click on the invisible triangles called "pass triangles".

d) **M.Eluard** [29] proposed a scheme "**Click-A-Secret**" which is a combination of both Locimetric and Cognometric schemes. Initially, user have to create an image by replacing some regions of an original image. These regions are called Gecu (Graphical element chosen by User). During the time of registration, user has to click on Gecu of an image and then validates the image to create password. During the login, user clicks on the Gecu of the initial image, then later finds all his/her personal images. This scheme offers high security.

e) **Gao** proposed a scheme called **passhand**s is a combination of recognition based and palm based biometric technique [30]. This scheme uses image of palm of human. During the login phase, nine images are placed in 3x3 grid in which one of image is chosen as a password image. At the time of login, the Users have to compare left or right hand to that particular region which is generated by the system image and click on password image. It is tedious process to do hand comparison as it is time consuming.

f) **Click Buttons According to Figure in Grids(CBFG)** [31] is a scheme which combines Locimetric, Cognometric, and Alphanumeric scheme. During the time of registration, Users offered with four background images and ten icons. The user has to choose one cell as a password cell and also choose an icon as a password icon. The user has to keep clicking the remaining keys to ensure that the buttons are clicked.it provide a large password space as there are multiple background images in the CBFG.

III. SECURITY ATTACKS ON GRAPHICAL PASSWORD SYSTEMS

a) Dictionary Attack:

In this type of attack, an attacker tries to guess the password from a dictionary which is a collection of list of words. Dictionary consists of all passwords based on the previous selections and all the passwords have high probability. Thus, if a user chooses a password, which is present in the dictionary, then the attack is successful. This attack is based password brute forcing.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

b) Guessing Attack:

Many a times, user prefer to choose their passwords based on their personal information such as house name, phone number, etc... In most of these cases, the attacker tries to guess the password by accessing the user's personal information. Guessing attacks can be categorized into two: online password guessing and offline password guessing attacks. In online password guessing, the attack guesses a password by manipulating inputs of one or more than one oracles. In offline, password guessing attacker searches for the password through manipulation of inputs of one or more than one oracles.

c)Shoulder Surfing Attack:

In shoulder surfing attack, the attacker watches over the behaviour of the user based on the direct observation technique.one of the direct observation technique, is looking over the persons shoulder to trace the password. It usually occurs in public places.

d)Spyware Attack:

Spyware is kind of a malicious software installed onto user's computers with aim to steal information of users. The method to execute a spyware attack is either through key logger or key listener. This malware collects the information about the user without his/her knowledge and thus leak this information to an outsider.

e) Social Engineering Attack:

Social engineering attack takes place through human interaction which causes users to give out sensitive information. In this type of attack, the attacker fakes himself to be an employee of an organisation and tries to interact with user to collect information related to the organisation. The attacker does not use any kind of electronic gadget but with his/her own intelligence and tricky conversation to get information he/she want.

Knowledge based scheme		Schemes	Attacks				
			Dictionary attack	Guessing	Shoulder-Surfing attack	Spyware	Social Engineering attack
Recognition Based		Deja Vu	N	Y	Y	N	D
		Story	N	Y	Y	N	M
		Cognitive	Y	Y	Y	Y	D
		DAS	N	N	N	Y	M
		GPI	Y	N	N	Y	D
Recall Based	Recall Pure Based	Syukri	N	N	N	Y	M
		Passhapes	Y	N	N	Y	M
	Recall Cued Based	Passpoints	N	Y	N	N	D
		CCP	N	N	N	N	D
Hybrid		Passhands	Y	N	Y	Y	D
		CAS	Y	N	N	Y	D

TABLE I summarises the different knowledge based scheme. We analyse 'Y'mean yes,which resistant to attack,'N' means No which is open to attack. In case of Social Engineering'E'indicates easy to attack.'M' means middle i.e. difficult is medium level.'D' denotes attack s very difficult

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

IV. CONCLUSION

In this study, different techniques from recognition based, cued recall based and hybrid schemes of graphical password techniques are surveyed and reviewed. Although the main feature about graphical password is that users are able to memorize the graphical password than text-based passwords. Our preliminary analysis is that it is difficult to break the graphical password over the traditional attack methods such as brute force search, dictionary attack or spyware. Therefore, it can be concluded that there are common drawbacks on the graphical pass scheme. Also, we tried to survey the attack pattern and included some common attack. Finally, we make a comparison TABLE I among various graphical password authentication techniques based on the attack patterns.

REFERENCES

[1] A.Adams,and M.A Sasse,"Users are not enemy:why users compromise computer security mechanisms and how to make remedial measures.", Communications to make remedial measures , vol. 42, pp. 41–46, 1999.
[2] M 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,vol -3,June 2008.
[3] K. Gilhooly," Biometrics: Getting back to business", in Computerworld, May 09,2005.
[4] R.Dhamija and A.Perrig,"Déjà vu:A User Study using Images for Authentication",In Proceedings of the 9th Conference on USENIX Security Symposium,vol-9,pp 4,Aug 2000.
[5] M.Kotadia,"Microsoft:Write down Your Passwords",In ZDNet Australia,May 23,2005.
[6] Christopher Mallow,"Authentication Methods and Techniques",pp 695-697,2007.
[7] http://www.iso.org/iso/catalogue_detail.html
[8] D.Florencio and C.Herley,"A Large-scale of WWW Password Habits",In 16th Proceedings ACM International World Wide Web Conference(www),pp 657-667,May 2007.
[9] K.Renaud and E.Smith Jiminy,"Helping user to Remember their Passwords",Annual Conference of South African Institute of Computer Scientists and Information Technologists,Pretoria,South Africa,pp 25-28,2001.
[10] H.C.Gao,X.Y.Liu,S.D Wang,R.Y.Dai,"A New Graphical Password Scheme against Spyware by Using CAPTCHA",In Proceedings of 5th Symposium on Usable Privacy and Security,Article no:21,July 2009.
[11] Sacha Brostoff,M.Angela Sasse,"Are Passfaces More Usable than passwords?:A Field Investigation",In Proceedings of HCI 2000,Jan 2000.
[12] W.Jansen,S.Gavrila,V.Korolev,R.Ayers,R.SwanStrom,"Picture Password:A Visual Login Technique for Mobile Devices",In National Institute of Standards and Technologies Interagency Report,vol NISTIR 7030,2003.
[13] Davis.F.Monrose and M.K Reiter,"On User Choice in Graphical Password Schemes",In Proceedings of 13th USENIX Security Symposium,vol-13,pp 11,Aug 2004.
[14] Sobardo,L and Birget,J,"Graphical Passwords",The Rutgers Scholar,An Electronic Bulletein of Undergraduate Research,Ruthgers University,New Jersey,vol-4,2004.
[15] S.Man,D.Hong and M.Mathews,"A ShoulderSurfing Resistant Graphical Password Scheme,"In proceedings of International Conference on Security and Management,vol-1,June,2003.
[16] K.Bicakci,N.B.Atalay,M.Yuceel,H.Gurbaslar,and B.Erdeniz,"Towards Usable Solutions to Graphical Password Hotspot Problem",In 33rd Annual IEEE International Computer Software and Application Conference,0730-3157/09,July 2009.
[17] I.Jermyn,A.Mayer,F.Monrose,M.K.Reiter and A.D.Rubin,"The Design and Analysis of Graphical Passwords",In Proceedings of the 8th USENIX Security Symposium,vol-8,pp 1,Aug 1999.
[18] J.Thorpe and P.C.Van Oorschot,"Graphical Dictionaries and The Memorable Space of Graphical Passwords",In Proceedings of the 13th USENIX Security Symposium,vol-13,pp 10,Aug 2004.
[19] Christopher Varenhorst,"Passdoodles:A Lightweight Authentication Method",MIT Research Science Institute,July 2004.
[20] R.Weiss and A.De.Luca,"Passhapes Utilizing Stroke Based Authentication To Increase Password Memorability",In Proceedings of the 5th Nordic Conference on Human-Computer Interaction ,Oct 2008.
[21] Ali Mohamed Eilejtlawi,"Study and Development of a New Graphical Password System,May 2008.
[22] G.Blonder,"Graphical Password",In Lucent Technologies,Inc.Murray Hill,NJ,United States Patent,5559961,1996.
[23] S.Wiedenbeck,J.Water,J.Birget,A.Brodskiy and N.Memon,"Passpoints:Design and Longitudinal Evaluation of a Graphical Password system",International Journal of Human-Computer Studies,vol-63(issue 1-2),pp 102-127,2005.
[24] Passlogix http://www.passlogix.com,Accessed on February 2007.
[25] S.Chiasson,P.C.Van Oorschot and R.Biddle,"Graphical Password Authentication Using Cued Click Points",In European Symposium on Research in Computer Security(ESORICS),LNCS 4734,pp 359-374,Sept 2007.
[26] S.Chiasson,A.Forget,R.Biddle and P.C.Van Oorschot,"Influencing Users Towards Better Passwords:Persuasive Clicked Points",In 8th proceedings of the 22nd British HCI Group Annual Conference on People and Computers:Culture,Creativity,Interaction,vol-1,pp 121-130,2008.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

[27] H.C Gao,X.Y Liu,S.Wang,R.Dai,"A New Graphical Password Scheme Against Spyware by Using CAPTCHA",In Proceedings of the Symposium on Usable Privacy and Security,pp 760-767,2009.
[28] H.Zhao and X.Li,"S3PAS:A Scalable Shoulder-Surfing Resistant Textual Graphical Password Authentication Scheme",In 21st International Conference and Advanced Information Networking and Application Workshops,vol-2,pp 467-472,2007.
[29] Elaurd,M.Maetz.Y,Alessio.D,"Action-Based Graphical Password:Click-A-Secret",IEEE International Conference on Consumer Electronics,pp 265-266,2011.
[30] H.C Gao,L.C Ma,J.H Qiu and X.Y Liu,"Exploration of hand based Graphical Password Scheme",Proceedings of the 4th International Conference on Security of Information,pg 143-150,2011.
[31] X.Y.Liu,J.H Qiu,L.C Ma,H.C Gao,."A Novel Cued-Recall Graphical Password Scheme",International Conference on Image and graphics(ICIG),vol-6,pp 949-956,2011.