Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 2, February 2015, pg.247 – 254

SURVEY ARTICLE

Graphical Passwords Authentication: A Survey

Nikhil Tarkeshwar Ambade[1], Prof. Dr. Arati Dixit[2]

[1]M.E. student, Department of Computer Engineering PVPIT, Shavitribhaiphule Pune University, India

[2]Professor, Department of Computer Engineering PVPIT, Shavitribhaiphule Pune University, India

[1] Nikhil.ambade50@gmail.com; [2] Adixit98@gmail.com

Abstract*— *In typically text-based passwords, well known users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. Reusing same or easy passwords across different accounts help to memorability, but decrease in security. Text passwords are the most popular user authentication method, but have security and usability problems. Alternatives such as biometric systems and tokens have their own drawbacks Graphical passwords offer another alternative. This paper conducts a comprehensive survey of the existing graphical password techniques also classifies these techniques into three categories: recall, recognition, and cued-recall approaches. This paper discusses security and usability aspects of graphical password techniques and point out the future research directions in this area.

Keywords*— *Graphical password, Authentication, Text passwords, Security, Usability

I. INTRODUCTION

An authentication is an assurance that the entity is one that claims to be. Authentication is any protocol or process that permits one entity to establish the identity of another entity [4].The main purpose of authentication schemes is to allow system access only by legitimate users. Authentication methods can be divided into three main categories [2] as shown in Figure 1:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication

Token based technique is an authentication method in which tokens such as key cards, bank cards and smart cards are used to provide security. Many token-based Authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number.

Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition. This technique uses hardware which is expensive. The major drawback of this approach is that such systems can be costly 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. Graphical password systems are a type of knowledge-based authentication that attempt to leverage the human memory for visual information which reduced memory burden that will facilitate the selection and use of more secure or less predictable passwords, discourage users from unsafe coping practices.

II. GRAPHICAL PASSWORD TECHNIQTES

The drawbacks of text based password are stolen the password, forgetting the password, and weak password. Therefore, a necessity to have a strong authentication method is needed to secure all our applications. Traditionally, conventional passwords have been used for authentication but they are known to have security and usability problems. Graphical password have been proposed as a alternative to text-based password, motivated by the fact that humans can remember pictures better than texts. Figure 2 help to understand graphical password technique and their aspects throughout the paper.

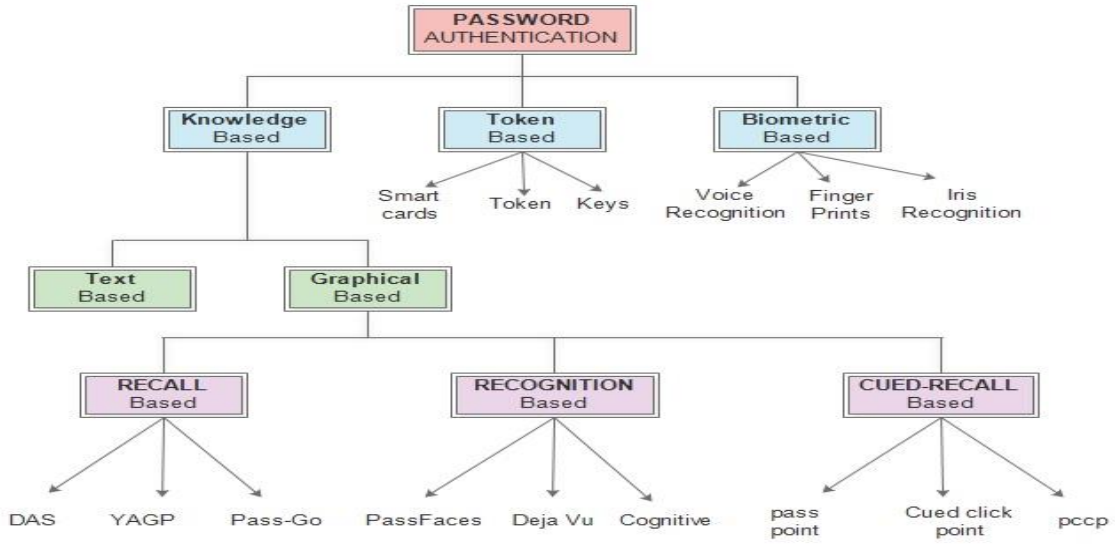


Figure 1: Categories of password authentication.

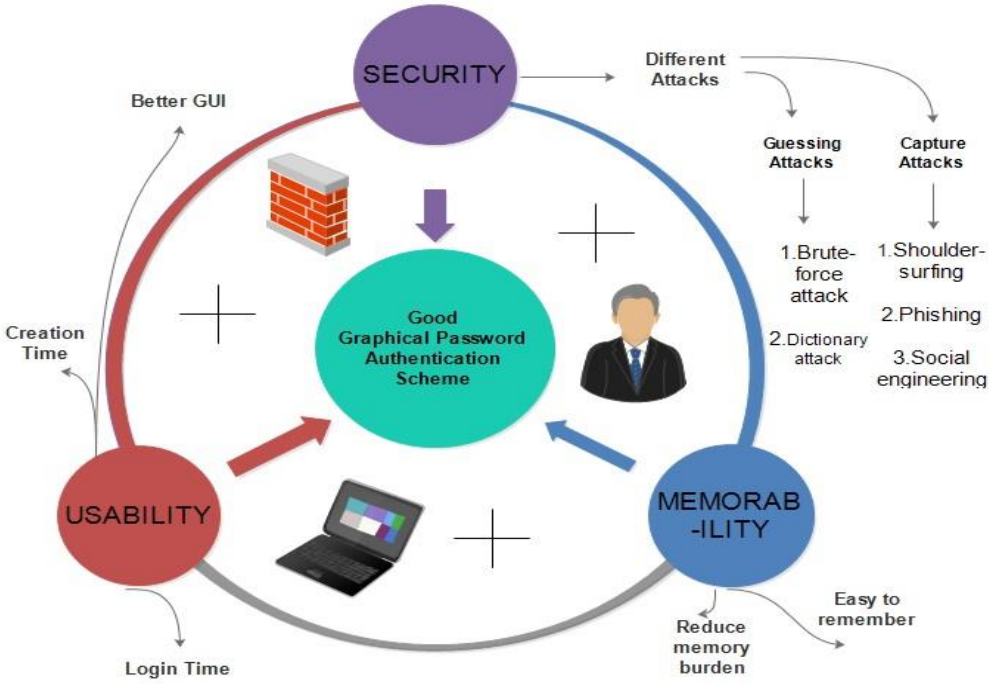


Figure 2: Understanding Graphical password and their aspects.

Graphical passwords can be broadly categorized according to the memory task involved in remembering and entering the password: recall, recognition, and cued-recall [1].

A. *Recall-based graphical password systems*

In this system users recall and reproduce a secret on image. The user has to reproduce something that he/ she created or selected earlier during the registration stage. The graphical password scheme retrieval is done without memory prompts or cues and attacks possible are shoulder-surfing, Phishing attack.

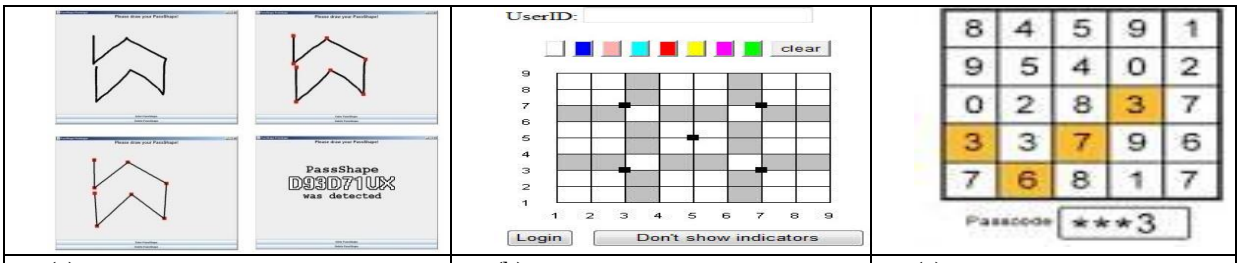
1. Techniques of Recall-based system

Draw-A-Secret (DAS) is a recall based graphical system which allows users to use a set of gestures drawn on a grid to authenticate. User's drawing is mapped to a grid & co-ordinate pairs used to draw the password in order and theoretical password space of DAS is 2^58 [8]cardinality for 5 × 5 grid and length 12.Background Draw a Secret (BDAS) is an extended form of DAS. The same grid is used as the original Draw a Secret, but a background image is simply shown over the grid. Added background images to DAS to encourage users to create more complex passwords. Dunphy and Yan [14] compared DAS to BDAS scheme and they found success rate of DAS as 57-80%.YAGP (Yet another Graphical Password) is a modification to DAS. In YAGP Approximately correct drawings can be accepted. The main drawback of YAGP is that it's hard to redraw the password precisely. Pass-doodle is another recall based system allows users to create a freehand drawing as a password (see Figure 3-c). It is similar to DAS and it uses more complex matching process without a visible grid and characteristics such as pen colour, number of pen strokes, and drawing speed.

(a) (b) (c)

Figure 3: Recall-based system (a) Draw-A-Secret [14] (b) BDAS [16] (c) Pass-doodle [16]

Pass shapes (see Figure 4-a) system based on 8 stroke directions Passwords are translated into alphanumeric characters and recognized at 45 degree intervals. During login, Pass Shapes can be drawn in a different size or location on the screen and still be translated into correct output provided the stroke direction is accurate. Pass-Go is a graphical password scheme motivated by DAS usability issue, in which a user selects intersections on a grid as a way to input a password. Pass-Go is the only recall-based graphical password system to date for which testing in a field study has been reported. Results of the 167 participant study showed that login success rates were acceptable at 78%, no login times were reported. GrIDsure (see Figure 4-c) is a product displays digits in a 5 x 5 grid. Users have to select and memorize a pattern consisting of an ordered subset of the 25 grid squares, and enter the corresponding digits therein using a keyboard. The system store the user's pattern itself in a recoverable manner to allow verification of the user's input, which will vary across logins. In a study [19] users achieved a login success rate of 87% with passwords of length 4.



(a) (b) (c)

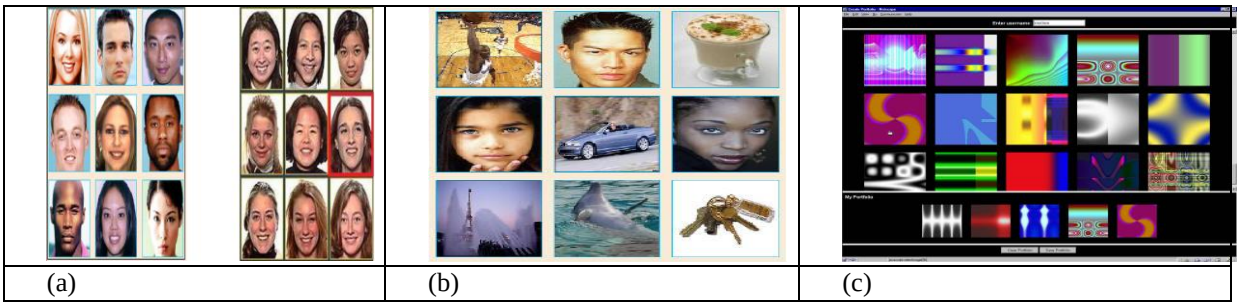
Figure 4:Recall-based system (a) Pass-shapes [17] (b) Pass-Go [1] (c) GrIDsure [18]

B. *Recognition-based graphical password system*

Recognition based systems also known as cognometric systems [3] or search metric systems generally require that users memorize a portfolio of images during password creation, and then to login, must recognize their images. It involves identifying previously seen images. The user must only be able to recognize previously seen images and not able to generate them unaided from memory. This technique has been proposed using various types of images. Attacks possible are Man-in-the-middle (MITM) attack, Shoulder-surfing attack.

1. *Techniques of Recognition-based system*

In Pass-faces [13] recognition based system users pre-select a set of human faces (see Figure 5-a).During login, a panel of candidate faces is presented. Users must select the face belonging to their set from among decoys. Several such rounds are repeated with different panels. For successful login, each round must be executed correctly. The set of images in a panel remains constant between logins, but images are permuted within a panel, incurring some usability cost. Davis et al. [15] conducted a study where he found that user's selected predictable passwords that could be easily guessed by attackers. In Story system users first select a sequence of images for their portfolio. To login, users must identify their portfolio images from among decoys. Users must select images in the correct order .Users were instructed to mentally construct a story to connect the everyday images in their set. In Déjà vu [10] system (see Figure 5-c) users select and memorize a multiple random art images from a larger sample for their portfolio. To login, users must recognize images belonging to their pre-defined portfolio from a set of decoy images.



(a) (b) (c)

Figure 5: Recognition-based system (a) Pass-faces [1] (b) Story system [1](c) Déjà vu [1]

In Cognitive scheme [12] Keyboard input is used rather than a mouse and users must recognize images from their previously memorized portfolio. The login task involves computing a path through a panel of images starting from the top-left corner, based on whether particular images belong to the user's portfolio: move down if you stand on a picture from your portfolio, move right otherwise. Users perform several rounds, each on a different panel. When the probability passes a certain threshold, login succeeds. This tolerates some user error. In a user study, 95% login success rate is reported. In VIP (Visual Identification Protocol) system pictures are uses instead of numbers as a means for user authentication. In this system a panel of images is displayed. Users must select images from their portfolio among decoys. Different configurations allow for multiple rounds or sequencing of images. VIP was found to provide a promising and easy-to-use alternative to the PIN. The visual code is easier to remember, preferred by users and potentially more secure than the numeric code. Photographic authentication [11] is a technique for logging into entrusted public Internet access terminals. It requires a user to identify their own personal photographs from a set of randomized images. In the Convex Hull Click Scheme (see Figure 7) users select and memorize a portfolio of images, and must recognize these images from among decoys displayed, over several rounds. The images are small icons and several dozen are randomly positioned on the screen. Each panel contains at least 3 of the user's icons. Users must identify their icons, visualize the triangle they form, and click anywhere within this triangle. This scheme protects against shoulder-surfing, but comes at a cost of longer login times. In Graphical Password with Icons (GPI) and Graphical Password with Icons suggested by the System (GPIS) users have to log in by selecting their 6 icons in an order from a panel of 150 icons. GPI allows users to choose any 6 icons as their password. In GPIS, passwords are suggested by the system but users may shuffle until they find an acceptable password, reducing problems with user choice.

Figure 6: Cognitive Authentication [2]

Figure 7: Convex Hull Click Scheme [2]

C. *Cued-recall graphical password system*

In a cued recall based graphical password systems, users identify and target previously selected locations within one or more images. User is provided with a hint to recall his password and images itself act as memory cues to aid recall. This feature intended to reduce the memory load on users and is an easier memory task than pure recall. Attacks possible in this system are Man-in-the-middle (MITM) attack, Shoulder-surfing, Malware attack.

1. Techniques of Cued-recall system

In pass point technique, password contains sequence of click points on a given image. The image is divided into tolerance squares. Users can select any points on the image as password in any order during registration stage. To login to the system the users have to correctly click on the same points in the image in correct order which is in the same tolerance squares as entered in the registration stage. The main drawback of this technique is pattern attack and brute force attacks are possible. Wiedenbeck et al. [5] conducted user studies on Pass Points. It required 171 seconds of training time on average to memorize their password. Users took 64 seconds to create a password, and Login took between 9 and 19 seconds on average.

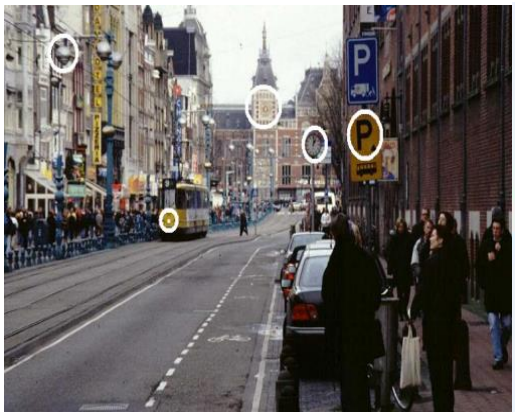


Figure 8: Pass Points

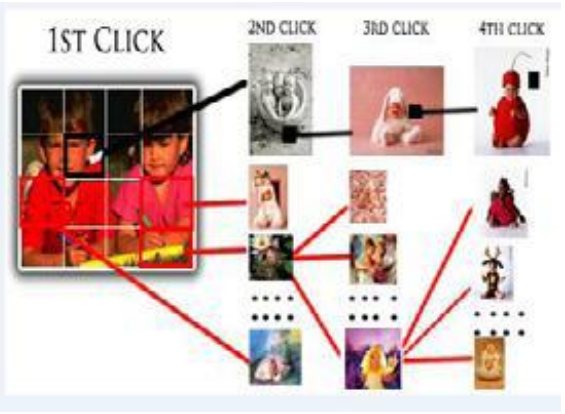


Figure 9: Cued Click-Points

In Cued Click-Points (CCP) method users have to click on one point per image on five different images shown in sequence. To create a different password users have to click on different click points in different images. This method provides implicit feedback which will be useful only to the legitimate users. While logging on users must have to click on the same click points in the sequence of image. If any of the click points selected by the user is not correct, authentication failure is indicated after selecting the final click point only. A user navigates through images to form a CCP password. Each click determines the next image of graphical passwords is available elsewhere. In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues to aid recall. Although Pass Points is relatively usable security weaknesses make passwords easier for attackers to predict. Hotspots are areas of the image that have higher likelihood of being selected by users as password click-points. Attackers who gain knowledge of these hotspots through harvesting sample passwords can build attack dictionaries and more successfully guess Pass Point passwords. Remembering the order of the click-points is no longer a requirement on users, as the system presents the images one at a time. User study [6] of CCP shows, users successfully logged in on the first time, in

96% of trials. On average, participants took 25 seconds to create a password, and 7 seconds to login. User testing and analysis showed no evidence of patterns in CCP, so pattern-based attacks seem ineffective. Although attackers must perform proportionally more work to exploit hotspots, results showed that hotspots remained a problem.

Persuasive cued click point (PCCP)[7] work like CCP, but during registration the images are slightly shaded except for a small selected area (viewport).PCCP is designed to persuade users to select more random passwords. PCCP encourages users to select less predictable passwords. A password consists of the image which is shaded except for viewport that is randomly positioned on the image. Users select a click-point within this viewport or may press a "shuffle" button to randomly reposition the viewport until a suitable location is found. On login, images are displayed in their normal format with no shaded or viewport. In a lab based study [7], login success rates were similar to CCP. On average it took 50 seconds to create a password and 8 seconds to log in. The Persuasive Cued Click Points scheme is effective at reducing the number of hotspots while still maintaining usability. This system has the advantage of reducing the formation of hotspots across users since click points are more randomly distributed at the time of password creation users may shuffle as often as desired but it slows the process of password creation.

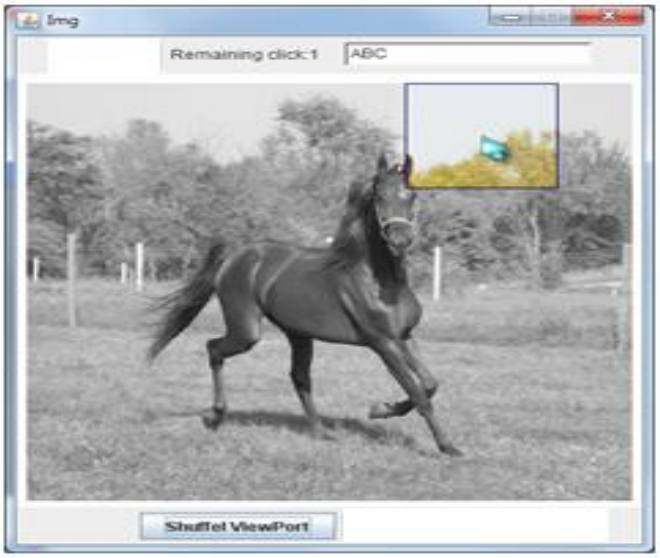


Figure 10: Persuasive cued click point

III.USABILITY AND SECURITY GOALS

The empirical study was designed to explore important usability and security goal in authentication systems. Usability should be explored along several dimensions. For usability, essential elements to measure and report include: time to create a password, and time to login. Allowing users to select their own password can aid usability since a password having personal meaning may be easier to remember. But it has also disadvantage that user choice leads to predictable patterns that can exploited by attackers. Allowing users to use their own images may improve memorability and encourage positive affective responses [8], but predictability and personalization may weaken security like in PassFaces system. It is unlikely that any single scheme will suit all domains tasks, and target users, from a combined usability and security viewpoint. Thus, specifying the target environments and applications for newly proposed schemes is important. Usability should be evaluated jointly with an exploration of their impact on security, since a usable authentication system without adequate security fails to meet its primary purpose. For example, a system where users can choose memorable-but-weak passwords may be usable but can provide a false sense of security. Table 1,2, and 3 shows the comparisons of above discussed Graphical passwords schemes based on the literature survey. The success rates are the number of trails completed without errors or restarts.

Table 1: Recall-based systems (summary)

Scheme	DAS	BDAS	YAGP	PassDoodle	PassShapes	PassGo	GrIDsure
Create Time							
Login Time					6 s		
Success Rate	57-80%	50-80%	87-96%	38-46%	63-100%	78%	87%

Table 2: Recognition-based systems (summary)

Scheme	PassFaces	Story	Déjà vu	Cognitive	VIP	Photo-graphic	Convex HullClick	GPI/GPIS
Create Time								
Login Time	14-88 s		32-36 s	90-180 s	5-6 s	40 s	72 s	18-19 s
Success Rate	72-100%	85%	90-100%	>95%	11-95%	95-100%	90%	83-74%

Table 3: Cued-recall systems (summary)

Scheme	PP	CCP	PCCP
Create Time	64 S	25 S	50 S
Login Time	9-19 S	25 S	8 S
Success Rate	38-94%	96%	83-94%

The security analysis of Recall based graphical password schemes are only gave the usability and weak security. This showed that a significant proportion of the DAS password space depends on the assumption that users will choose long passwords with many composite strokes. Thus successful dictionary attacks [1] on Pass-Go and DAS require less effort than initially expected. Further study is required to determine how complexity properties like grid dimensions, password length, and number of composite strokes impact memorability and user choice in passwords.

After comparing different methods of graphical password authentication it looks that usability and security are work in inversely proportional way. If one likes to make memorable graphical password system it reduces the security, for example, adding extra rounds to Passfaces increases security but also increases an additional memorability. Above tables shows the success rate, creation time and login time of each methods studied from different papers. By analysis this data it shows that password creation time and login time takes different time which affects the usability of system. Now the challenge for the next generation of graphical passwords schemes is to designs new schemes and architectures which afford increases in security and usability together.

IV. CONCLUSION

The discussion for graphical passwords schemes shows that people are better at remembering picture passwords than text based passwords. This papers preliminary analysis suggests that we need to improve our authentication systems to be more reliable, robust and secure as there is always a place for improvement. A challenge for designers is to identify memory aids for legitimate users that cannot be leveraged by attackers to guess passwords. Much research on graphical password techniques need to be done to reach better levels of usefulness security.

References

1. R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM ComputingSurveys (to appear), vol. 44, no. 4, 2012.

2. XiaoyuanSuo, Ying Zhu, G. Scott, Owen, "Graphical Passwords: A Survey", Department of Computer Science, Georgia State University.

3. A. De Angeli, L. Coventry, G. Johnson, and K. Renaud." Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems".International Journal of Human-Computer Studies, 2005.

4. "Christopher Mallow "Authentication Methods and Techniques".

5. S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon."PassPoints: Design and longitudinalevaluation of a graphical password system". International Journal of Human-Computer Studies, 63(1-2):102 127, 2005.

6. S. Chiasson, P. C. van Oorschot, and R. Biddle."Graphical password authentication using Cued ClickPoints". In European Symposium On Research In Computer Security (ESORICS), LNCS 4734, September 2007.

7. S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot."Inuencing users towards better passwords: Persuasive Cued Click-Points". In Human Computer Interaction (HCI), The British Computer Society, September 2008.

8. M. Mannan, T. Whalen, R. Biddle, and P. van Oorschot."The usable security of passwords based on digital objects: From design and analysis to user study". Technical Report TR-10-02, School of Computer Science, Carleton University, 2010.

9. Passfaces Corporation. The science behind Passfaces.White paper, http://www.Passfaces.com/ enterprise/resources/white_papers.htm, accessed July 2009.

10. R. Dhamija and A. Perrig. "Deja Vu: A user study using images for authentication". In 9th USENIX Security Symposium, 2000.

11. T. Pering, M. Sundar, J. Light, and R. Want."Photographic authentication through untrusted terminals". Pervasive Computing, January - March 2003.

12. D. Weinshall. "Cognitive authentication schemes safe against spyware (short paper)". In IEEE Symposium on Security and Privacy, May 2006.

13. S. M. Bellovin and M. Merritt. "Encrypted key exchange: Password based protocols secure against dictionary attacks". In IEEE Symposium on Research in Security and Privacy, 1992.

14. P. Dunphy and J. Yan. "Do background images improve Draw a Secret" graphical passwords?" .In14th ACM Conference on Computer and Communications Security (CCS), October 2007.

15. D. Davis, F. Monrose, and M. Reiter. "On user choice in graphical password schemes".In 13th USENIXSecurity Symposium, 2004.

16. Source :http://www.google.co.in/imagesearch:. Downloaded on 19 November 2014.

17. Source : http://www.google.co.in/imagesearch:. Downloaded on 23 November 2014.

18. Source : http://www.gridsure.org/GrIDsure.jpg. Downloaded on November 2014.

