International Conference on Innovative Applications in Engineering and Information Technology(ICIAEIT-2017)

International Journal of Advanced Scientific Technologies ,Engineering and Management Sciences (IJASTEMS-ISSN: 2454-356X) Volume.3,Special Issue.1,March.2017

Recall Based Authentication System- An Overview

P. Baby Maruthi[1], Dr. K. Sandhya Rani[2]
[1]Research Scholar: Dept of Computer Science
S.P.M.V.V, Tirupati, Andhra Pradesh, India
[2]Professor: Dept of Computer Science,
S.P.M.V.V, Tirupati, Andhra Pradesh, India

Abstract - Even today, in many applications textual passwords are used as a traditional approach of authentication. These textual passwords are not secured and could be easily guessed. Moreover textual passwords might be gained with the techniques such as brute force, dictionary attacks, social engineering, and shoulder surfing and spyware attacks. Therefore, information is not secured by using textual passwords as a method of authentication. To overcome these problems, graphical passwords authentication is evolved as an alternative method for textual password. In this graphical password authentication, images are used as passwords in place of text, because images are easy to remember than text. A graphical password consists of clicking images or drag the images, or rotating the images as a password and not typing the text in textual passwords. Generally, graphical password techniques are categorized into three main categories: recall based, recognition based and hybrid based. In Recall based techniques, user has to reproduce a drawing without giving any hint as a password. In recognition based technique, user has to select or recognize the images from different sets of images and that image is same as the image selected at the time of registration phase. In hybrid based technique, the combination of two more techniques involved in recall based or recognition based technique or both. Recall based techniques are classified into two categories: pure recall based technique and cued recall based technique. In this paper, various categories of recall based techniques and various algorithms applied in recall based techniques are presented and compared.

Keywords - Graphical Passwords, Recall Based, Pure Recall Based, Cued Recall Based

I. Introduction

Authentication is a process which provides and confirms the identity of a person. It is the process of giving someone identity so that he or she can access that particular application or data. Authentication systems are broadly classified in to three major categories. They are token based, biometric based and knowledge based authentication systems.

In token based authentication, hardware tokens are generally produced as small and easy to carry devices. Bank cards, key cards and smart cards are commonly used as tokens. These tokens are used as a method of authentication for doing safe transactions or keeping information secure.

Biometric Based Authentication is a process that validates the identity of a user to sign in into a system by measuring some intrinsic characteristics such as DNA, fingerprints, iris scan, facial recognition, voice, etc. [1].

Knowledge based authentication requires the knowledge of private information of the user to prove that the person providing information is the owner of the identity. In this paper, an overview of recall based authentication which belongs to knowledge based authentication system is presented.

II. Knowledge based Authentication

In this scheme, the knowledge of information is provided by the user to prove the identity of a person. By supplying the information about the user identity, while login to the system, he/she may prove that information given at the time of registration phase is same as at the login phase. Knowledge based authentication is generally classified into two categories: text based password authentication and graphical password authentication as shown in the Fig 1.

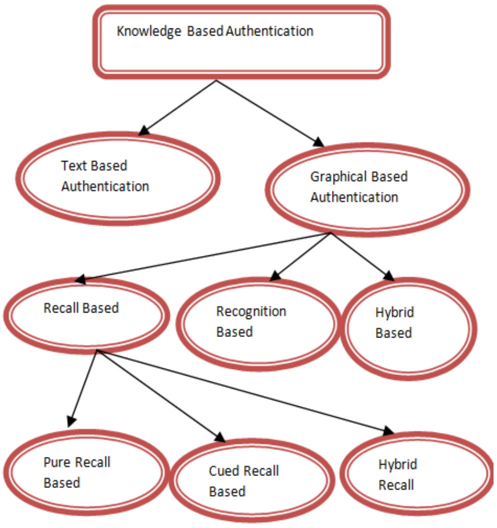


Fig 1: Knowledge Based Authentication

2.1 Text Based Password Authentication

The most traditional approach of authentication is text based authentication. In textual password authentication, user provides a secret word or phrase consisting of alpha-numeric characters to authenticate the system. These passwords are not highly secure. Because textual passwords are generally the user created most memorable strings such as their mobile numbers, names or their birth day dates, etc. These passwords can easily stolen by the attacker by using various techniques such as brute force, spyware, social engineering, shoulder surfing etc. and also there may be a chance of forget their password. To overcome the drawbacks of text based authentication, an alternative solution is graphical password authentication.

2.2 Graphical Password Authentication

In graphical password authentication [10], identifying the images or produce something to draw rather than the text to authenticate the owner of the identity. In this scheme, recognizing the pictures is usually a password rather than the text in text based authentication. There are two important aspects in graphical passwords. Firstly, graphical passwords are easy to memorize and secondly, they are more efficient to enter and there are many other factors like usability and security. The main advantage of graphical password authentication is more secure than the text based password authentication.

In this paper, a brief description of graphical password authentication systems is presented. The three major categories of authentication systems are: Recall based, recognition based and hybrid based authentication systems. The various techniques which belong to these categories are also discussed in this paper.

In recognition based authentication systems, the user has to select an image or picture from a large collection of images in the database in the registration phase and the same image or picture has to recognize while login to the system.

In recall based Authentication System; user is asked to reproduce something as a password without giving any hint. An overview of recall based authentication system is given in the following section 3.0.

In hybrid based systems, a combination of two or more recall or recognition based authentication techniques are used to identify the person.

III. Recall based Authentication

Recall is the procedure of the human nature to remember what was done or what was the event. In this scheme, user has to draw some shapes such as circle, square etc., at the time of registration phase. While login to the system, user has to produce the same pattern on the two dimensional grid.

Recall based authentication techniques are classified into three main categories namely; pure recall based, cued recall based and hybrid recall based. The overview of pure recall based, cued recall based and hybrid based techniques are presented in the following sections.

3.1 Pure recall based

In pure recall based authentication system, user has to reproduce or draw something as their password without producing any hint at the time of login phase. The widely used pure recall based techniques are Draw-A-Secret, Syukri, and Pass doodle are described in the following sub sections.

❖ Syukri

Syukri [4] is one of the techniques in pure recall based authentication system. In this system, user is able to draw a signature by using a mouse. This technique involves two stages namely, registration and verification. In the registration stage, user is asked to draw a signature using mouse and the system extract signature either by enlarge or scale down the signature and rotates if needed. This information stored in the database. The sample output of Syukri algorithm as shown in the Fig3.

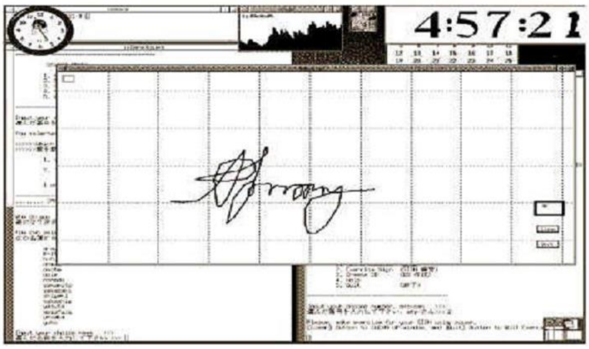


Fig 2: Syukri algorithm

In the verification stage, input takes signature does normalization and exacts the different parameter of signature. The advantage of Syukri algorithm is no need to memorize one's signature and it is hard to forge other's signature. The disadvantage of this technique is drawing a signature using mouse is difficult and can be used pen like devices as light pen rather than mouse but expensive.

❖ Pass doodle

Goldberg et al. proposed a technique called pass doodle [7]. In this technique, user has to draw hand written designs or text on a stylus sensitive touch screen. Some of the pass doodles drawn by the user as shown in the Fig4.

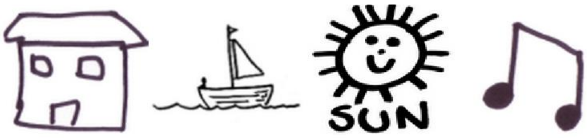
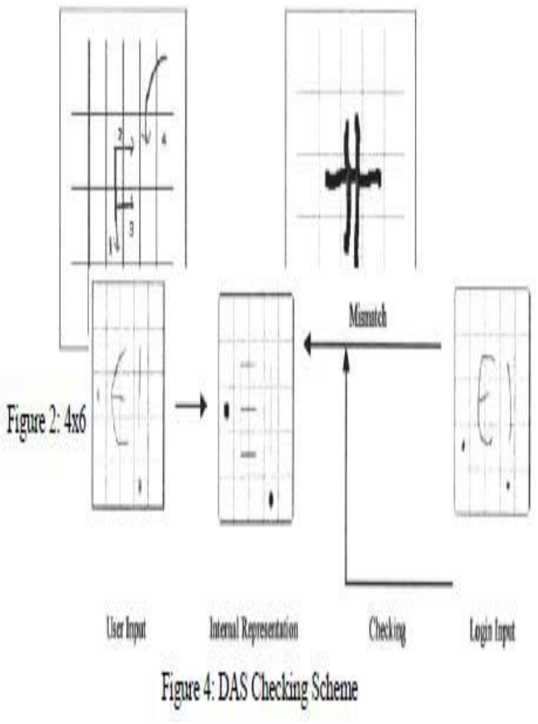


Fig 3: Pass doodle

When login to the system, user has to draw the same pass doodle which was already drawn at the registration phase.

❖ Draw-A-Secret

Draw-A- Secret (DAS) scheme was proposed by Jermyn [8], user is asked to draw their own password. User has to draw password on a two dimensional grid touches on a stylus sensitive touch screen. When the user is available to login to the system, user has to draw the same shape and also strokes that touch on the grid must be the same which has been already drawn at the registration phase, then the user is authenticated. The sample output of DAS scheme as shown in the Fig 4.



3.2 Cued recall based

In cued recall based authentication system [6], the user has given some clues or hint implicitly to produce their passwords at the time of login stage. The widely used cued recall based techniques are Blonder, Pass points and cued click points are described in the following subsections.

❖ Blonder

Blonder technique developed by Greg E [9]. Blonder in which a pre determined image shown to the user and user should locate or pointed to two or more regions on the predetermined image. In Fig5, user selected tap regions in predetermined image.

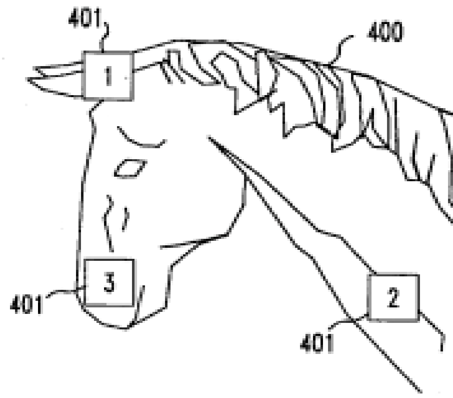


Fig 5: Blonder

The drawback of this technique is the number of clickable points position is relatively small, so the password becomes quite long to secure.

❖ Pass point

Pass point scheme was proposed by wiedenbeck et al [2] [13]. In this scheme, the user has to select several click points in an image with some order during at the time of registration phase. While login to the system, user has to select the same click points with the same order that the user has been selected the same sequence of click points chosen at the registration phase. The user selected sequence of click points on the image as shown in the Fig 6.

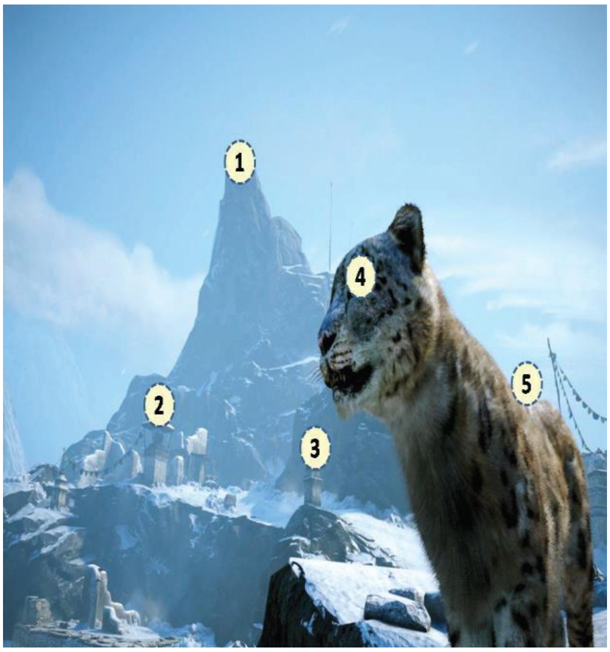


Fig 6: Pass point

The disadvantage of pass point scheme is login time is longer than the usual password.

❖ Cued Click Points

To overcome the drawbacks of pass point scheme, cued click points scheme was proposed. The main difference between the pass point scheme and the cued click points [3] scheme is one click point on one image rather than all click points on the same image. The user has to select click point on one image and next click point on the other image with some sequence. While login to the system, the user has to follow the same sequence and then the user is authenticated. An example of cued click points as shown in the following Fig 7.

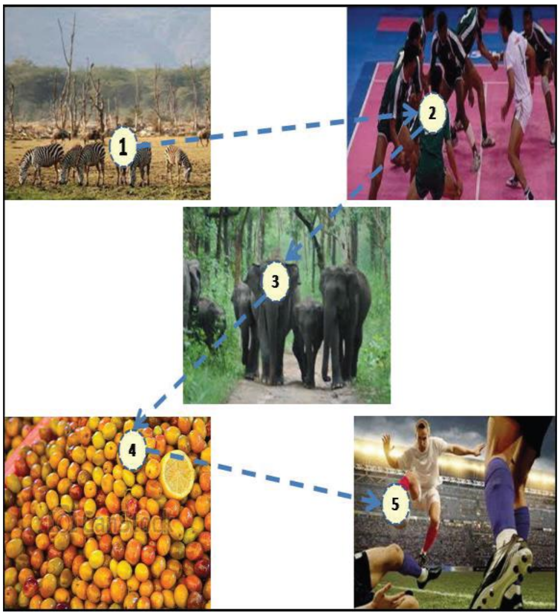


Fig 7: Cued Click points

3.3 Hybrid Recall based Systems

In this system, the combination of one or more schemes in pure recall based and also cued recall based techniques are used for hybrid recall based authentication.

❖ Click Draw based - Graphical Password Scheme (CD- GPS)

In this scheme, the combination of DAS in pure recall based technique and cued click points scheme in cued recall based technique is introduced. A set or collection of images in the database is called image pool. It consists of several themes of ten different images such as fruits, landscape, cartoon characters, food, sport, buildings, cars, animals, books and people. In this image pool, the user has to select only four images in a story sequence (i.e. the sequence of actions of images take part as per the selection of images chosen by the user and these actions of images easily memorized by the user) and the users may construct and remember their own stories as per the image selection. For example, out of ten images in the image pool, the user has to select only four images as shown with the number 6,3,4,7 in the Fig 8.

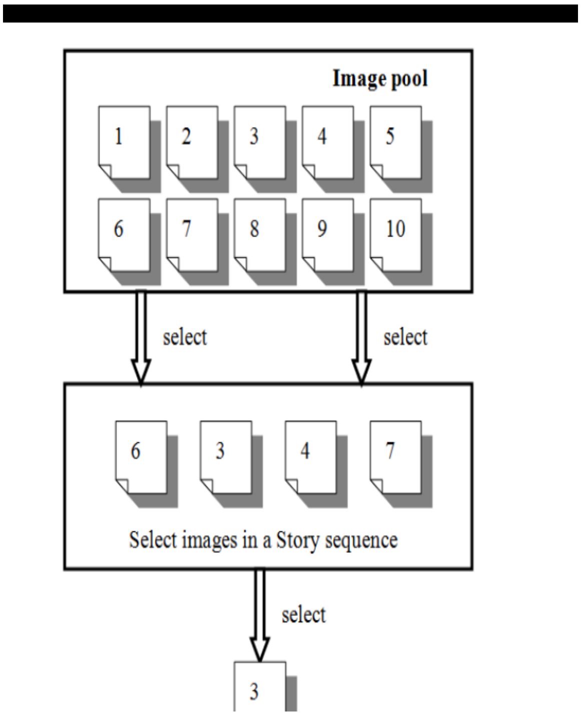


Fig 8: Image selection

Again, the user has to select only one image out of four images (6, 3, 4, 7) i.e. image 3 as shown in the Fig 8. User can draw the secret [5] on image during the final selection of the image. In Fig.9, the user click-drew a digital number of 'T' as the secret, which consists of coordinates (13, 3), (13, 4), (13, 5), (14, 4), (15, 4) and (16, 4).

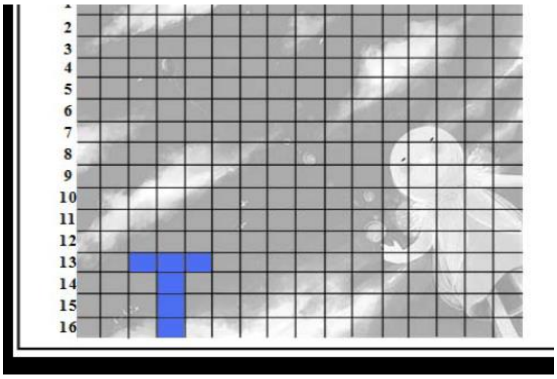


Fig 9: CD-GPS

Therefore, during the authentication, users should reproduce their secrets accurately in the correct coordinates on their selected images but without the need to consider and remember the click order [11].

Usability and Security The features of usability and security in recall based authentication systems could increase the user to select the better selection of passwords and also increase the effectiveness of password space.

Table 1: Usability and Security features of various recall based authentication systemThere are different recall based graphical password techniques measured in terms of usability and security aspects as shown in the following Table 1[11][12].

Techniques	Usability			Security issues	
	Authentication process	Memorability	Resistant to attacks	Password space	Possible attacks
DAS	User draw a graph on a 2D grid	Drawing sequence is hard to remember	Brute force, Spyware	Low password space	Dictionary attack, shoulder surfing
Syukri	Draw signatures using mouse	Very easy to remember, but hard to recognize	Brute force, spyware	Infinite password space	Guess, dictionary attack, shoulder surfing
Pass doodle	Draw something with a stylus onto a touch sensitive screen	Depends on what users draw	Brute force, spyware	Infinite password space	Guess, dictionary attack, shoulder surfing
Blonder Pass point Cued Click points	Click on several pre-registered locations of a picture in the right sequence	Can be hard to remember	Brute force, spyware	N^K, N is the number of pixels units of the picture, K is the number of locations to be clicked on	Guess, brute force search, shoulder surfing
CD GPS	Choose image on a set of images and draw a secret on image.	Drawing a secret on image is easy to remember	Brute force, spyware, Guess	Infinite password space	Shoulder Surfing

IV. Conclusion

In this paper, recall based graphical password authentication schemes and various techniques that are widely used in pure recall based and cued recall based authentication systems are presented. The comparison of each technique in terms of usability and security also presented.

References

[1] Vashek Mathyas, Zdenek Riha, “Security of biometric authentication system,” International Journal of Computer Information System and Industrial Management Application, 2011.

[2] S.Wiedenbeck, J.Waters, J. Birget, A. Brodskiy, and N. Memon, “PassPoints: Design and longitudinal evaluation of a graphical password system,” International Journal of Human-Computer Studies, 2007.

[3] Vaibhav Moraskar, Sagar Jaikalyani, Mujib Saiyyed, Jaykumar Gurnani, Kalyani Pendke, “Cued Click Point techniques for graphical password authentication,” International Journal Of Computer Science And Mobile Computing, Vol.3 Issue.1, January- 2014, pg. 166-172.

[4] A.F. Syukri, E. Okamoto, and M. Mambo, “A user identification system using signature written with mouse,” *In: Proceedings of Australasian Conference on Information Security and Privacy (ACISP).* London, UK: Springer-Verlag, 1998, pp. 403–414.[5] D. Paul and J. Yan, "Do background images improve Draw a Secret graphical passwords?" , Proceedings of the 14th ACM conference on Computer and communications security, ACM, 2007.

[6] Karen Renaud, “On user involvement in production of images used in visual authentication”. Elsevier, Journal of Visual Languages and Computing, 2008.

[7] Christopher Varenhorst, “Passdoodles; a lightweight authentication method ”, Massachusetts Institute of Technology, Research Science Institute, July 27,2004.

[8] Jermyn Ian, A. Mayer, F. Monrose, M. K. Reiter and A. D. Rubin,“The design and analysis of graphical passwords”, Proceedings of the Eighth USENIX Security Symposium. August 23-26 1999. USENIX Association 1–14, 1999.

[9] Susan Wiedenbeck, Jean-Camille Birget, Alex Brodskiy; “Authentication using graphical Passwords: effects of tolerance and image choice”, Symposium On Usable Privacy and Security (SOUPS), Pittsburgh, PA, USA, 2005.

[10] Ali Mohamed Eljetlawi, “Study and Develop a New Graphical Password System”, University technology Malaysia, Master Dissertation, 2008.

[11] Yuxin Meng, “Designing Click-Draw Based Graphical Password Scheme for Better Authentication”, IEEE Seventh International Conference on Networking, Architecture, and Storage, 2012.

[12] Xiaoyuan Suo, “A Design and Analysis of Graphical Password”, (Department of Computer Science, George State University), 2006.

[13] Amol Bhand,vaibhav desale, Swati Shirke, Suvarna Pansambal (Shirke) “Enhancement of Password Authentication System Using Graphical Images” International Conference on Information Processing (ICIP) Vishwakarma Institute of Technology. Dec 16-19, 2015.