International Journal of Research
ISSN: 2348-6848 Vol-3, Special Issue-3
International Conference on Research and Recent Trends in Engineering and Technology. (ICRRTET)
Held on 27th January 2016 organized by **Sai Polytechnic College,** Kinhi Jawade, Yavatmal, Maharastra, India.

Survey Of Graphical Password Authentication Techniques

Nikita R. Dive; Manjiri D. Likhar; Nayana A. Ughade ; Samiksha S. Chune & Payal M. Khonde

Abstract
Now-a-days, user authentication is an important topic in the field of information security. To enforce security of information, passwords were introduced. Text based password is a popular authentication method used from ancient times. However text based passwords are prone to various attacks such as dictionary attacks, guessing attacks, brute force attacks, social engineering attacks etc. Numerous graphical password schemes have been proposed so far as it improves password usability and security. In this paper, we conduct a comprehensive survey of the existing graphical password techniques. We can categorize these techniques into four: recognition-based, pure recall-based, cued-recall based and hybrid approaches. Here we analyze the strengths and drawbacks of each method. This survey will be particularly useful for researchers who are interested in developing new graphical password algorithms as well as industry practitioners who are interested in deploying graphical password techniques.
Keywords- Graphical Password; Information Security; Password Usability; Security.

• INTRODUCTION

In recent years, information security has been formulated as an important problem. Main area of information security is authentication which is the determination of whether a user should be allowed access to a given system or resource. In this context, the password is a common and widely authentication method. A password is a form of secret authentication that is used to control access to data. It is kept secret from unauthorized users, and those wishing to gain access are tested and are granted or denied the access based on the password according to that.

Passwords are used from ancient times itself as the unique code to detect the malicious users. In modern times, passwords are used to limit access to protect computer operating systems, mobile phones, and others. A computer user may need passwords for many uses such as log in to personal accounts, accessing e-mail from servers, retrieving files, databases, networks, web sites, etc. Normal passwords have some drawbacks such as hacked password, forgetting password and stolen password[1]. Therefore, strong authentication is needed to secure all our applications. Conventional passwords have been used for authentication but they are known to have problems in usability and security. Recent days, another method such as graphical authentication is introduced. Graphical password has been proposed as an alternative to alphanumeric password. Psychological studies have shown that people can remember images better than text. Images are generally easier to be remembered than alphabets and numbers, especially photos, which are even easier to be remembered than random pictures [2].

In this paper, we conduct a comprehensive survey of the existing graphical password algorithms. We will discuss the strengths and drawbacks of each method and also proposes future scope in this area. In this survey, we want to answer the following questions:

- Are graphical passwords more secure than alphanumeric passwords?
- What are the major issues in implementation of graphical passwords?
- What are the limitations of various existing graphical password techniques?

This survey will be beneficial to information security researchers and practitioners who are interested in finding an alternative to text-based authentication methods.

Graphical based password techniques have been proposed to solve the limitations of the conventional text based password techniques, because pictures are easier to remember than texts. It is referred as "Picture superiority effect" [3]. A literature survey of papers regarding graphical password techniques shows that the techniques can be categorized into four groups as follows (Fig.1):

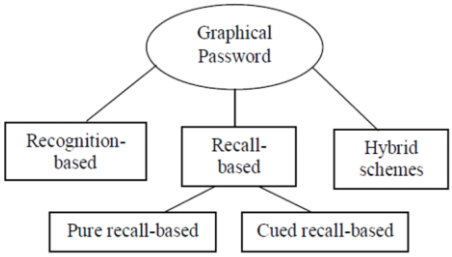

Fig.1. Categorization of Graphical password authentication techniques

- Recognition-Based Technique

In this category, users will select images, icons or symbols from a collection of images. At the time of authentication, the users need to recognize their images, symbols or icons which are selected at the time of registration among a set of images. Researches were done to find the memorability of these passwords and it shows that the users can remember their passwords even after 45 days [4].

- Recall Base Technique

  - Pure Recall-Based Technique

In this category, users have to reproduce their passwords without being given any type of hints or reminder. Although this category is very easy and convenient, but it seems that users can hardly remember their passwords. Still it is more secure than the recognition based technique.

  - Cued Recall-Based Technique

In this category, users are provided with the reminders or hints. Reminders help the users to reproduce their passwords or help users to reproduce the password more accurately. This is similar to the recall based schemes but it is recall with cueing.

- Hybrid Schemes

In this category, the authentication will be typically the combination of two or more schemes. These schemes are used to overcome the drawbacks of a single scheme, such as spyware, shoulder surfing and so on.

II. TECHNIQUES

- *Recognition based Systems*

Major headings are to be column centered in a bold font without underline. They need be numbered. "2. Headings and Footnotes" at the top of this paragraph is a major heading.

  - *Jensen et al. Method*

Jensen et al. [5] proposed picture password scheme for mobile PDAs in which user was asked to select a theme. Images of size 40 x 40 were shown in a 5 X 6 matrix on the basis of selected theme, User have to select images from the matrix with the help of stylus. A numerical sequence based on image selection is registered to form a password. At login time user has to recognize same images in same sequence at login time. Main flaw was that password space was small since, the no of images were limited to 30.

Fig. 2 Cats and dogs theme.

Fig. 3 sea and shore theme

- *Passfaces Method*

Real User Corporation developed a product called passfaces[6] it is supported by the fact that human brain can quickly recognize familiar faces. During registration user has to select 4 faces. The registration is complete if the user correctly identifies 4 passfaces two times consecutively. During login user is presented with a login screen consisting of grid of faces. User has to select 4 faces: one face from each of 4 grids of 9 faces. It has been cited by Davis et al. [7] Passfaces can be predictable as they are affected by race, gender and attractiveness.

Fig. 4 Passfaces Scheme.

- *Sobrado and Birget Method*

Sobardo and Birget [8] developed a method to prevent shoulder surfing attack. During registration user was asked to select objects from no of displayed objects. At login time the user has to select objects selected at registration time and then click inside the convex hull formed by objects. To make password space larger 1000 objects were used at login process. However, the display became crowded and it was difficult to find pass -objects.

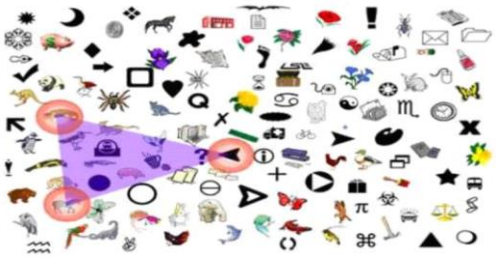
Fig. 5 convex hull shoulder surfing.

- *Hong et al. Method*

Hong et al. [9] proposed spyware resistant method in which at registration time the user is presented with a login screen divided in to grids each grid containing a icon. Each icon has no of variations (as shown in figure) .user has to select a pass-icons from the login screen .User has to enter a string corresponding to each variation of pass -icons. At login time user is challenged with recognizing the pass - icons from a n grid login screen containing no of icons. Each icon in grid is from variations of that icon. Once the icons has been correctly identified user has to enter string corresponding to the variation of particular pass - icon. Registration and login process in this scheme is time consuming.

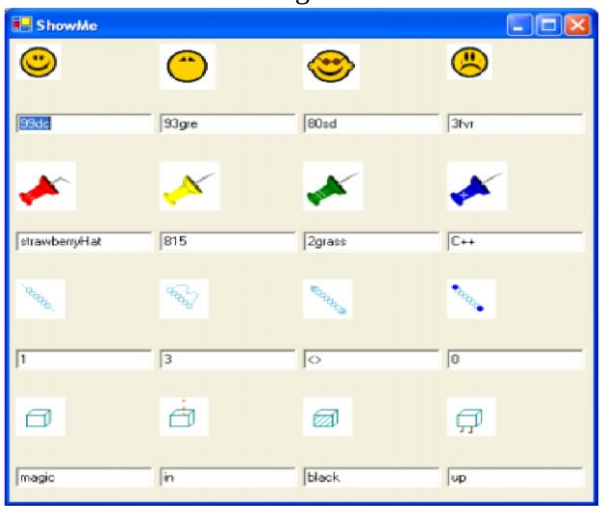

Fig. 6 Proposed beam former.

- *Recall based Systems*
- *Reproduce a Drawing*

Jemryn et al. [10] proposed a technique called" Draw asecret (DAS)".In this scheme during reg istration user has to draw something on a GRID of size Y X Y. The coordinates (X,Y) of the grid were stored in the order of drawing. To log in, user has to redraw such that the drawing touches the registered sequence of coordinates. This technique lead to increased password space, reduced traffic load, since images were not transferred over network.

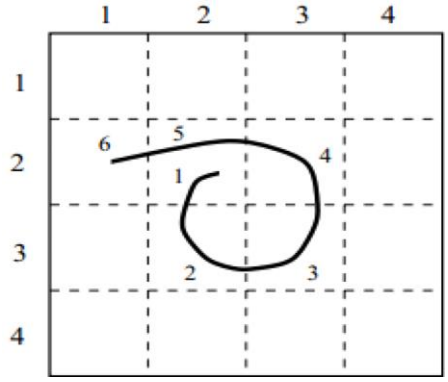

Fig. 7 Jermyn et al. DAS Scheme

- *Blonder Scheme*

G.E blonder [11] designed a scheme in which a image is presented to user with tap regions, for authentication user has to click within those tap regions and in a sequence. The major drawbacks of this scheme was memorable password space moreover, user cannot click where he wants because of predetermined tap regions.

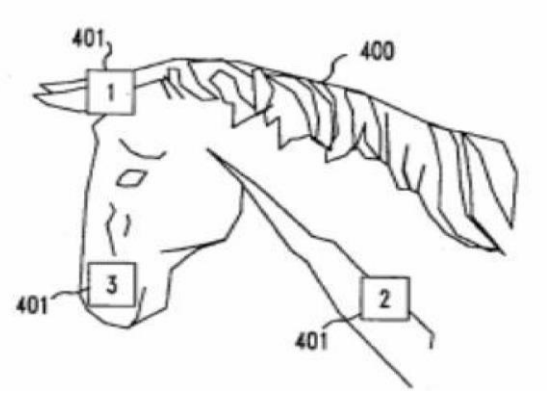

Fig. 8 Blonder Scheme

- *VisKey*

SFR company [12] developed a scheme for mobile devices user has to select an image from the images stored in the device and tap on the spots in sequence this sequence is registered. To login user has to tap at same spots as and should be in registered sequence. The Inputs are within a certain tolerance area around it pre-defined by users, since it is difficult to touch at same exact spots. If input precision is large password will be easy to crack on the other hand if it is small it will be difficult for the user to tap at exact points. In visKey no of spots must be larger to prevent against brute force attacks .

Fig. 9 visKey

- *Cued Click Points*

Unlike pass point rather than making multiple clicks on single image use has to make single click on multiple images. The images come in sequence one after the other. An image appearing next in sequence is determined by the click made in the previous image. The main advantage of this technique is cued recall and making click on single image results in larger password space and it is more resistant to shoulder surfing attack.

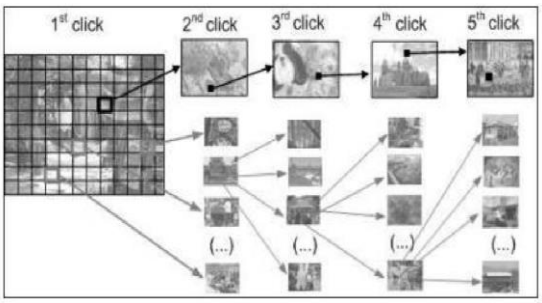

Fig. 10 Cued Click Points

C. HYBRID SCHEMES

Hybrid schemes are the combination of two or more graphical password schemes. These schemes are introduced to overcome the limitations of a single scheme, such as hotspot problem, shoulder surfing, spyware, etc. Many single schemes on recognition-based and recall-based schemes are discussed and some of these schemes are combined to develop the hybrid schemes.

Jiminy [4] proposed a hybrid scheme in which image is used as a reminder for helping users to choose easy to remember graphical passwords. In this scheme, based on the color, templates are given to the users that contain several holes. First, the user chooses an image, then selects a colored template, then clicks on a specific location inside the image, and then selects the position to place the template and stores the password. At the time of login, the users have to choose the right template, place it on the correct location on the image then enter the characters visible through the holes from top to bottom. Memorability of the passwords in this scheme is higher than text based password as this scheme only requires users to remember the correct location of template on the image. Gao et al. proposed a hybrid scheme [13] using CAPTCHA (Completely Automated Public Turing tests to tell Computer and Humans Apart). It retains all the advantages of graphical password schemes and CAPTCHA technology.

During the registration phase, users select the images as their password images. For authentication, user is required to differentiate the password images from decoys and complete a test by recognizing and typing the CAPTCHA string below every password images. This scheme is almost impossible to break but still spyware may affect this Hybrid scheme.

Zhao and Li [14] proposed a Textual-Graphical Password Authentication scheme (S3PAS) to resist the shoulder surfing attacks. This scheme combines advantages of both textual and graphical passwords and is resistant to shoulder-surfing, spyware and hidden-camera attacks. At the time of registration, user has to select a string *k* as the original textual password. Password length may vary on different environments and for different security requirements. During login, user has to find the original password in the login image and then click inside the invisible triangles, called "passtriangles", created by the original password.

M. Éluard et al. proposed a hybrid scheme, "Click-asecret" (CAS) [15] which combines both *Locimetric* and *Cognometric* schemes. This scheme allows input and record a secret though interaction with an image. First, users have to create a personal image by replacing some specific regions of the original image. These regions are called as Gecu(Graphical Element Chosen by User). This region has a specific graphical element present in the original image. During registration, the user clicks on Gecu in the original image, which is then replaced by an alternate version. When the user thinks the current image is ideal to create the password, and then the user validates the personal image, thus make it more secure. This process is repeated for several rounds generating the user password. During the login stage, the user must click on Gecu in the first image, until the finds all of his or her personal images. This scheme offers high security compared to other hybrid scheme. However, the usability is not good due to the limitation of its reduced password space. Gao et al. proposed another hybrid scheme PassHands [16], which is a combination of recognition-based graphical passwords and palm-based biometric technique. This scheme requires the processed palm images of human instead of usually using faces. During the login phase, nine identically

sized processed sub-images of the palm are placed in a 3×3 grid at random where one of the images is a password image and the many decoy images to cover up. At the time of login, the users compare their left or right hand to the particular region with the generated image and then click on the password image. However, the usability still remains as an issue in PassHands compared to other schemes and also log in will become a tedious task as the hand comparison process needs more time.

Click Buttons according to Figures in Grids (CBFG) [17], is another hybrid scheme which is a combination of Locimetric, Cognometric and alphanumeric schemes. At the time of registration, the user is presented with four background images and ten icons. The users have to select one cell on each image as password cells and choose one icon as password icon. The user can click on any key til the icon is the password icon. Then the user has to click on the numeric key, then for each password cell. When the authentication of password cells is done, the users have to continue clicking the remaining keys to ensure that all the buttons are clicked. There are multiple background images in the CBFG, hence it provides a large password space compared to other hybrid schemes. However, hotspot problem can occur in password cell selection of CBFG. Since the sequence entered each time is in pure random manner, it is still a difficult task for the hacker to guess the user password even if he or she records the entire login process with a hidden camera.

III. SECURITY ATTACKS IN GRAPHICAL PASSWORD SCHEMES

- *Dictionary Attack*

In this attack, an attacker tries to guess the password from a very large list of words, dictionary. Dictionary will be the collection of all high probability passwords based on previous selections. If a user chooses a password, a word already within the dictionary, then this attack will be successful. This attack is a specific type of the password brute forcing attack.

- *Guessing Attack*

Many users tend to select their passwords based on their personal information like the name of their pets, house name, phone number, passport number, etc. In these cases, the attacker tries to guess the password by trying the main password possibilities based on the user's personal information. Guessing attacks can be broadly classified into two categories: online password guessing attacks and offline password guessing attacks. In online password guessing attack, attacker tries to guess a password by manipulating the inputs of one or more oracles. In offline password guessing attack, attacker exhaustively searches for the password by manipulating the inputs of one or more oracles.

- Shoulder Surfing Attack

Shoulder surfing attack refers to attack the user passwords by using direct observation techniques. Main direct observation technique is looking over someone's shoulder, to get the password. Shoulder surfing attack mostly occurs in public places because it is really easy in a crowd to stand near someone and look at them entering a password or any secret key.

- Spyware Attack

Spyware is a type of malicious software which installed on computers with the aim of stealing secret information of users. Spyware attack is normally done by using a key logger or key listener. This malwares gathers information without user's knowledge about gathering and leak this information to an outside source of attacker.

- Social Engineering Attack

Social engineering is the attack, in which human gains the sensitive information from the human interaction. In this type of attack, attacker tries to obtain the information about an organization or computer systems from the user itself to act like an employee. The attacker

doesn't use any electronic techniques of hacking in this kind of attack as he or she uses only human intelligence and tricky conversation to get the information he wants. When attacker gets some of information from one source, then he or she may gather information from other sources within the same organization to get the complete information and add to his or her credibility.

IV. CONCLUSION

In this paper, we have studied different techniques of graphical password authentication such as, recognition-based, pure recall-based, cued recall-based, and hybrid schemes. During our observation, we identify several drawbacks which can cause attacks on user data. Therefore, we have studied the common drawbacks on these graphical password methods. Also find how to overcome these attacks. Then, we tried to survey on attack patterns and define common attacks in graphical password authentication methods. We also find that, some attacks can be prevent, but user must have to take care of prevention of certain attack such as social engineering attack and shoulder surfing attack.

REFERENCES

[1] 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. 2008.

[2] http://www.iso.org/iso/catalogue_detail.htm.

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

[4] K. Renaud and E. Smith. Jiminy: "Helping user to remember their passwords". *Technical report, School of Computing, Univ. of South Africa*, 2001.

[5] Jansen, W. Gavrila, S. Korolev, V. Ayers, R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices", NISTt NISTIR 7030, 2003

[6] Real User Corporation, Passfaces TM http://www.realuser.com, Accessed on January 2007.

[7] D. Davis, F. Monrose and M.K Reiter, "On User Choice in Grap hical Password Schemes", In Proceesings of the USENIX Security Symposium, California, 2004.

[8] Sobrado, L and Birget, J. "Grap hical Passwords", The Rutgers Scholar, An Electronic Bulletin of Undergraduate Research, Ruthgers University, New Jersey, Vol.4, 2004.

[9] D. Hong, S. M an, B. Hawes, and M . Mathews, "A p assword scheme strongly resistant to sp yware", In Proceedings of International conference on security and management, Las Vergas, NV, 2004.

[10] I. Jermyn, A. Mayer, F. Monrose. M. K. Reiter and A. D. Rubin, "The Design and Analysis of GraphicalPasswords", In Proceedings of the 8th USENIX Security Symposium, 1999.

[11] G. Blonder, "Grap hical Password", In Lucent Technologies, Inc., M urray Hill, NJ,United States Patent 5559961, 1996.

[12] SFR IT -Engineering, http://www.sfrsoftware. de/cms/EN/pocketpc/viskey/, Accessed on January 2007.

[13] 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 the* symposium on usable privacy and security, 15-17 July, 2009.

[14] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant TextualGraphical Password Authentication Scheme",*in 21st International* Conference on Advanced Information Networking and Applications Workshops, vol.2. Canada, 2007, pp. 467-472.

[15] Eluard, M.; Maetz, Y.; Alessio, D.; , "Action-based graphical password: Click-a-Secret", *2011 IEEE International Conference on Consumer Electronics*, 2011, pp.265-266.

[16] H.C.Gao, L.C.Ma, J.H.Qiu and X.Y.Liu, "Exploration of a Hand-based Graphical Password Scheme", *Proceedings of the 4th international* conference on Security of information and networks, 2011.

[17] X.Y. Liu., J.H. Qiu., L.C. Ma., H.C. Gao., etc., "A Novel Cued-recall Graphical Password Scheme", *In sixth International Conference on* Image and Graphics (ICIG), pp.949-956, 2011.