ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (15-25), Month: July - September 2015, Available at: www.researchpublish.com

Survey on Security and Usability of Knowledge Based Authentication Mechanism

[1]Neha Singh, [2] Nikhil Bomanwar

[1,2] Software Engineering, Veermata Jijabai Technology Institute, India

Abstract: **In today's Security Mechanism Authentication plays a vital role. Well known text-based password authentication systems that have various flaws in terms of is security and usability issues which in turn create problems to users .This lead to emergence of an alternative mechanism to overcome these drawbacks. Rather than typing textual characters, graphical passwords involves dragging or clicking on the pictures, are considered as alternative to prevent the problems that arise from textual passwords. In this paper, a comparative study of the Knowledge based system is performed specifying the pros and cons of each of them .We have also specified various usability and security features for further research perspectives in this area..**

Keywords: **Graphical Password, Recognition, Authentication, Recall, Security.**

I. INTRODUCTION

In our day to day life most common and widely adopted technique in knowledge-based authentication mechanism is textual password. Although this traditional technique has several vulnerabilities that are well known to us. One of the major drawback is the difficulty of remembering passwords. It has been concluded through various studies that users tend to pick short passwords that are easy to remember which in turn help attacker to gain access of them through brute force attack, Dictionary attack, Guess, spyware etc. Whereas passwords that are hard to break or guess are often difficult to remember. Various studies have proved that human can only remember limited number of textual passwords, because of that limitation users either write down their password in plaintext form or use a single password for various kinds of applications. Goal behind improving the existing user authentication mechanism is to make it more secure and usable for the user. Graphical authentication system is proposed as an alternative to traditional text-based password techniques based on fact that pictures can be remembered better than text by humans as well as graphical passwords is difficult to guess or broke by brute force. Graphical password space may exceed in comparison to textual password if the number of possible images is sufficiently large, there forth providing better resistance to dictionary attacks. Due to above mentioned advantages, graphical password have gained rapid interest which have been implemented and applied to websites ,login applications, ATM machines, personal digital assistants (PDAs).

II. RELATED WORK

Authentication is defined as the process which positively verifies the user identity, device, or other entity in a computer system, in order to allow access to resources in the system. Traditional Authentication [1] .system is divided into three major categories which are as follows

1) Object Based Authentication

2) ID Based Authentication

3) Knowledge Based Authentication

1) Object-Based Authentication (Token)*:*

Object-Based Authenticators ("what you have")- They are characterized by physical possession. A physical token that is difficult to copy or forge is used by Token [4] based authentication. USB tokens, Bluetooth tokens magnetic, strip cards, or smart cards are examples of authentication token which refers a physical device that a individual carries around and uses in authenticating process.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (15-25), Month: July - September 2015, Available at: www.researchpublish.com

PROS: Tokens are cost-effective, portable, and secure.

CONS: Token is highly vulnerable to loss or theft so possession of a valid token is not proof of Legitimate user leading to leakage of confidential and important credentials of authorized users. Moreover, whenever access is required the user should have the token. This leads to emergence Of some better and secure authentication mechanism.

2) ID-Based Authentication (Biometrics):

ID-Based Authenticators ("who you are") They are characterized by uniqueness to one person. A driver's license, passport, credit card, etc, all fall in this category. Similarly Biometric [4] based authentication makes use of some unique features of a human to authenticate legitimate users, such as a voiceprint,fingerprint, iris scan, or signature. For both ID documents and biometrics, the important security defense is that they are difficult to forge or copy .

PROS: High accuracy is provided by Biometric-based authentication. Moreover the "password" cannot be easily stolen, forgotten, or given to another individual, thereby providing the highest level of security .There is no need for users to remember or carry the passwords when system access is required.

CONS: It may require costly devices to obtain and process the unique characters of individuals. The authentication process may be time-consuming. It sometimes locks valid users out. Due to this type of authentication is not yet widely adopted. Hence, in the remaining section, we focus on knowledge-based authentication which seems to eliminate the drawbacks of the previous authentications

3) Knowledge Based Authentication (Password)*:*

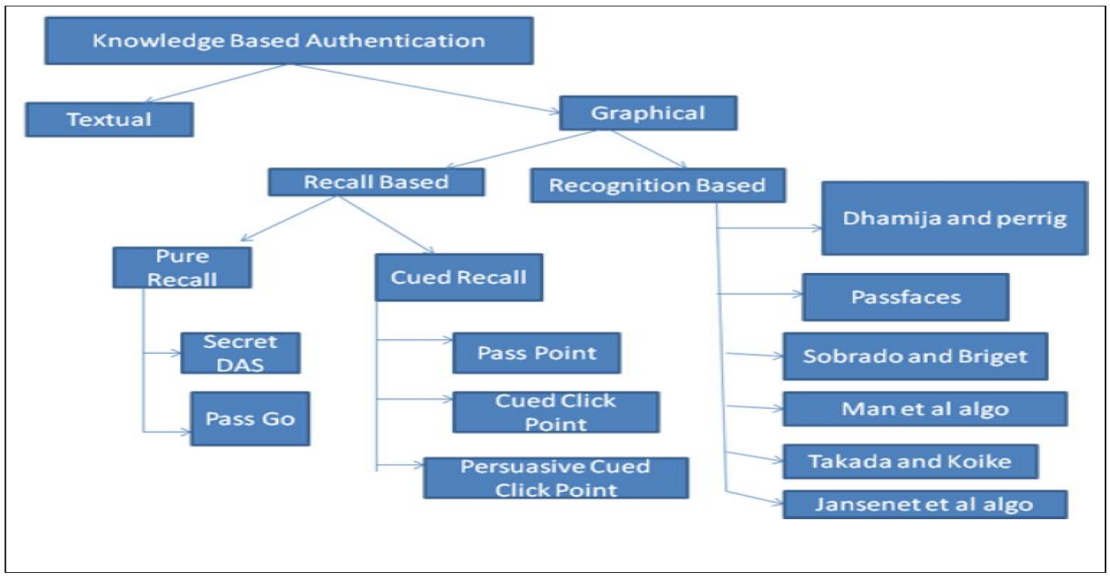
Knowledge-Based Authenticators ("what you know")— They are characterized by secrecy or obscurity. Knowledge based authentication type includes the memorized password. They can also consist of information that is not much secret. Today, most widely used authentication technique is knowledge-based authentication which makes use of password to prove identity and gain access to a resource. There are classified into two kinds of passwords: alphanumeric passwords and graphical passwords.

a) Textual Password (Alphanumeric passwords):

Traditionally, textual passwords are widely used authentication to protect user's privacy in computer and network.

PROS: Text based authentication take less time for the processing and usually occupy less space in memory. Text Passwords are easy to remember for users.

CONS: Simple user assigned passwords or memorable passwords are not secure they can be easily hacked by attackers through brute force attack, Dictionary attack, Guess, spyware etc. Strong System assigned passwords are difficult for users to remember so they turn to write them on some paper which also leads to certain security issues. Textual password space is less.



Fig(1) Classification Of Knowledge BasedAuthentication

b) Graphical Password:

The idea of graphical passwords was originally developed by Greg Blonder in the year 1996. Alternative authentication method to alphanumeric passwords is Graphical passwords[2] in which users click on images to authenticate themselves rather than typing textual password .Graphical passwords have been designed to make passwords more memorable and easier for people to use. Graphical Password is categorized into Recognition based and Recall based technique.

PROS: Graphical passwords are resistant to guessing, dictionary attack, key loggers, and social engineering. Graphical Password space is larger than textual password space.

CONS: In comparison to textual password, Graphical password occupies much larger space in memory and it requires more time for processing .Graphical passwords are vulnerable to shoulder surfing problem, and usability issues.

i) RECOGNITION BASED TECHNIQUE:

Recognition systems [5], also named as *cognometric* or *searchmetric systems which* generally require that users select and memorize a portfolio of pictures during password creation they must recognize and identify their images they have selected earlier during authentication process. Recognition based technique is divided into following category which are:

a) Passface algorithm

b) Dhamija and Perrig algorithm

c) Sobrado and Birget algorithm,

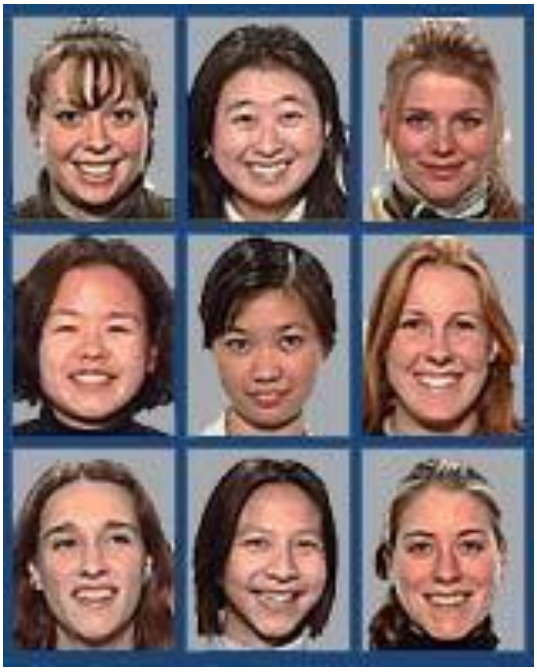
d) Jansen et al. algorithm,

e).Man, et al. algorithm.

f) Takada and Koike

a) Passface:

Passface [7] concept was developed by Real User Corporation based on the assumption that its easier for humans to recall human faces in comparision to other pictures. Under this technique during login user is presented a panel of candidate faces Fig(2)among which Users require to select the face belonging to their set. Repeatedly several such rounds are carried on with different panels. Each round needed be executed correctly for successful login.



Fig(2) Pass face

PROS: Pass faces password is easier to remember compared with textual passwords

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (15-25), Month: July - September 2015, Available at: www.researchpublish.com

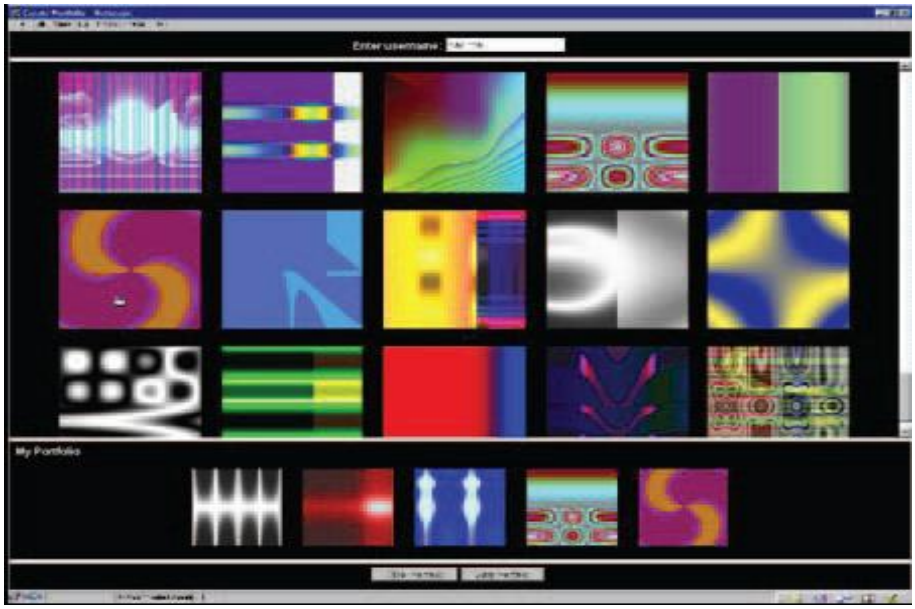
CONS: Passfaces cannot be used by people who are face-blind. Passfaces take longer time to login than textual passwords. Davis et al (2004) did Comparative studies and showed that, users choice is highly affected by user gender or race and attractiveness of the faces in Passfaces thereby making the Passfaces password predictable by the attackers.

(b) DHAMIJA AND PERRIG ALGORITHM:

Dhamija And Perrig Algorithm is based on Hash Visualization technique. From certain number of images (Figure 3) user will be asked to select few random pictures which are generated by a program. After which, for authentication pre-selected images need to be identified by user

Pros: Authentication using Dhamija and Perrig technique has a much smaller failure rate in comparision to textual Password.

Cons: In comparision to traditional approach the average log-in time is longer. A drawback is that the server needs to store a large amount of pictures which may have to be transferred over the network, delaying the authentication process.



Fig(3) Dhamija And Perrig

(c) Sobrado and Birget:

Sobrado and Birget proposed graphical passwords schemes that is resistant to shoulder-surfing attacks which includes Triangle Scheme, Moveable frame Scheme,Special geometric configuration Scheme .

i) First scheme Known as **"triangle scheme"**, a user needs to select their passobject among many displayed object. During the registration phase for authentication, a user needs to recognize all the preselected pass-object which was selected. Users need to select point inside the convex-hull formed by the pass-object

Triangle **Moveable** **Intersection**

CONS: The password space entirely depends on number of objects. If number of objects, is increased the display becomes more crowded thereby making it difficult to find the passobject. Reducing the number of objects , reduces the size of password space thereby making it easier to crack as well as guess.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (15-25), Month: July - September 2015, Available at: www.researchpublish.com

Table(1) Sobrado and Birget Schemes

SOBRADO AND BIRGET		
1st Scheme(Triangle scheme)	2nd Scheme(moveable frame scheme)	3rd Scheme(special geometric configuration)
Three passobjects	Three passobjects	Four passobjects
Password Space entirely depends on number of objects,increasing them makes display crowded and making it difficult to find the passobject, reducing them make it easy to guess and crack.	Repeating the process number of times by rotating or clicking it randomly makes process unpleasant, confusing and time consuming due too many non-pass objects.	To be authenticated, user only required to click the object nearest to the intersection point.

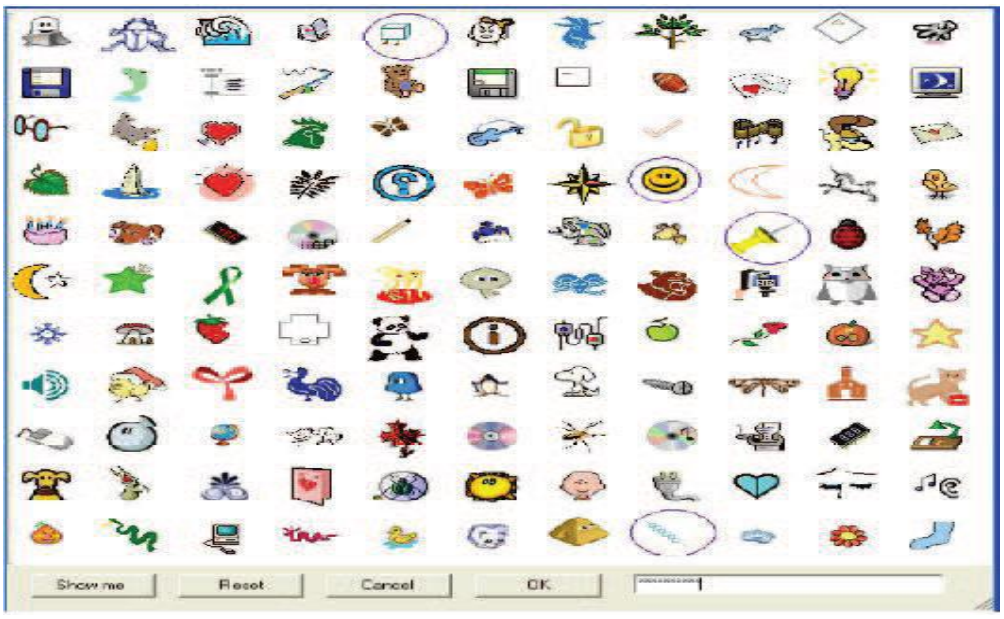
ii) Second scheme called **"moveable frame scheme"**. One of the pass-objects is placed into the moveable frame. To be authenticated, unless all the pass-object are located in a straight line the user requires to rotate the frame.

CONS: To minimize the probability of logging, they suggest clicking or rotating process randomly several times which is confusing ,unpleasant, and time consuming since too many non-pass objects exist.

iii) Sobrado and Birget last scheme is called **"special geometric configuration"**. In this scheme four passobjects are involved to form an intersection point. To be authenticated, object nearest to the intersection point is to be clicked by user

(d) MAN, ET AL. ALGORITHM:

Shoulder-surfing resistant algorithm, was proposed by Man, Et Al proposed in which a user choose number of pictures as passobjects having several variants each with unique code. During authentication user has to face many scenes , each scene contains several pass-objects and many decoy-objects. The user requires to type in a string with the unique codes corresponding to the pass-object variants present in the scene as well as a code indicating the relative position of the pass-objectswith respect to a pair of eyes.

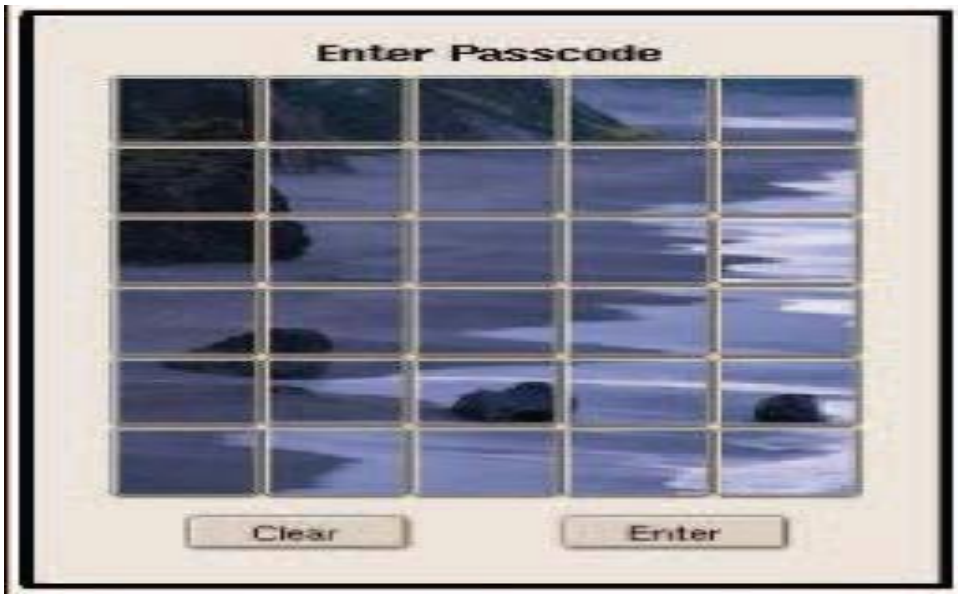


Fig(4) Man, Et Al

(e) JANSEN ET AL. ALGORITHM:

Jensen et al (2003) proposed a graphical password scheme based on "picture password" especially for mobile devices such as PDAs. For creation of password, a theme needs to be selected by user consisting of thumbnail photo after which ,they need to select and register a sequence of the selected thumbnail photo. For authentication user requires to identify and recognize previously seen photos by touching it by via stylus in the correct sequence.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (15-25), Month: July - September 2015, Available at: www.researchpublish.com



Fig(5) Jensen et al

CONS: Only 30 thumbnail photos is allowed, thereby reducing the size of the password space. Increasing password space , will make the selection of password more complex and difficult.

(f) TAKADA AND KOIKE:

Favourite image of users can be used by users in this technique for authentication. Initially users register their favorite images with the server. Several rounds of verification are required during authentication. During each round, among several decoy-images user selects a pass-image or chooses nothing if no passimage is present. If all verifications are successful. then only the program would authorize a user

PROS: Since users register their own images it makes easier for them to remember their pass images.

(i) RECALL-BASED SYSTEMS:

Recall-based graphical password systems also known as *drawmetric systems* because a secret drawing is recalled and reproduced by users. In these systems, users draw their password on a grid or canvas. Recall is difficult memory task, since retrieval is carried out without memory cues or prompts.

CONS: Shoulder surfing Attack, Social engineering Attack and Phishing Attack are possible to take place in recall based System.

(a) Draw A Sequence

(b) Pass Go

(c) Pass Point

(d) Cued Click Point

(e) Persuasive Cued Click Point

(a) Draw A Sequence:

Jermyn et al. proposed a scheme, known as"Draw-A-Secret [6] (DAS)" based on a two dimensional grid, in which users require to draw something to represent their password and each of the grids coordinates is stored in the order drawing was made. For authentication (Fig 6) , user needs to redraw the picture with the proper sequence at the same grids coordinates, then only user is authenticated

PROS: Users is provided freedom to draw a password as long as they wish moreover there is no need to transferr images through network thereby reducing traffic loads, and the server side graphical database storage. Password space of grid based schemes is better than traditional textual passwords,.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (15-25), Month: July - September 2015, Available at: www.researchpublish.com

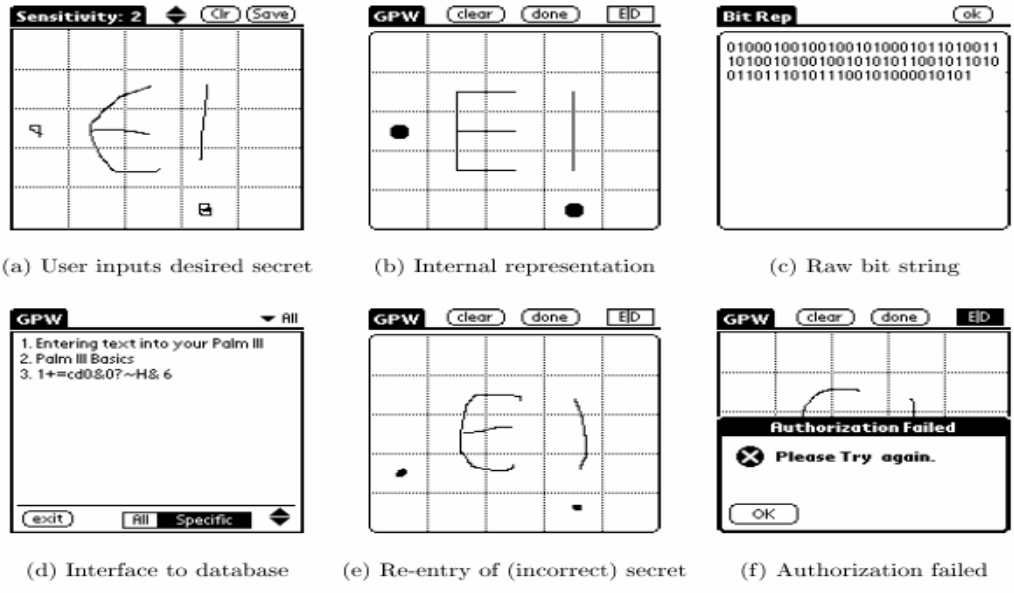
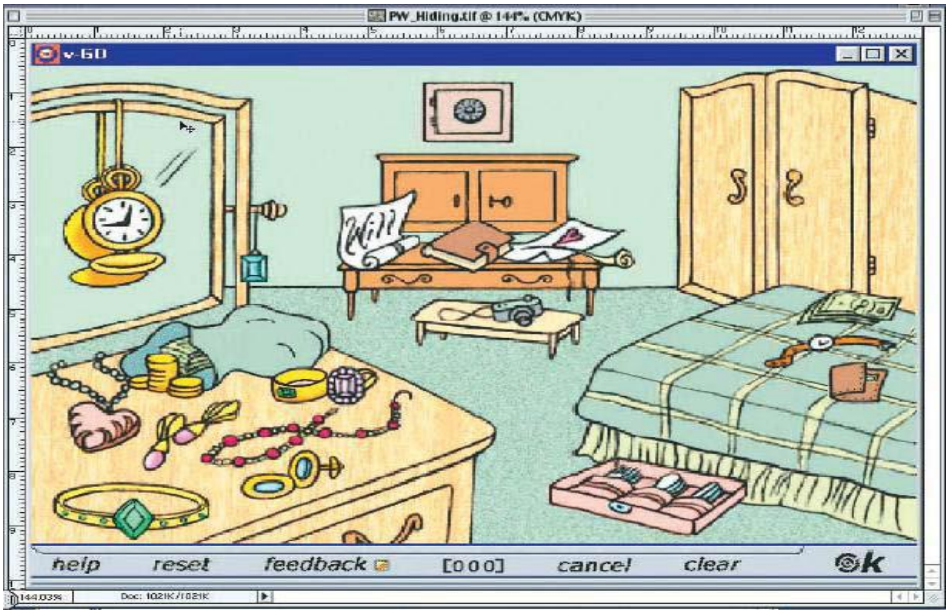


Fig (6)Draw A Sequence

CONS: It is vulnerable to guessing attack, shoulder surfng attack.

(b) Pass Go:

Passlo gix v-Go uses a technique known as "Repeating a sequence of actions". Based on the environment user can select their background images,(eg bedroom, kitchen, bathroom, or etc). User can click or drag on a series of items within that image to enter a password.



Fig(7):Pass Go

CONS: Size of password space is small thereby making them vulnerable to guessing attack.

(c) Pass Point:

In PassPoints [3], a password is created by clicking five click-points in a sequence on a given image (Figure 8). Users can select click-points as any pixels in the image for their password. For successfull log in, user repeat the sequence of clicks in the correct order, within a system defined tolerance square of the original click-points.

PROS: Password space is relatively large compared to textual passwords.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (15-25), Month: July - September 2015, Available at: www.researchpublish.com

Fig(8)Pass Point

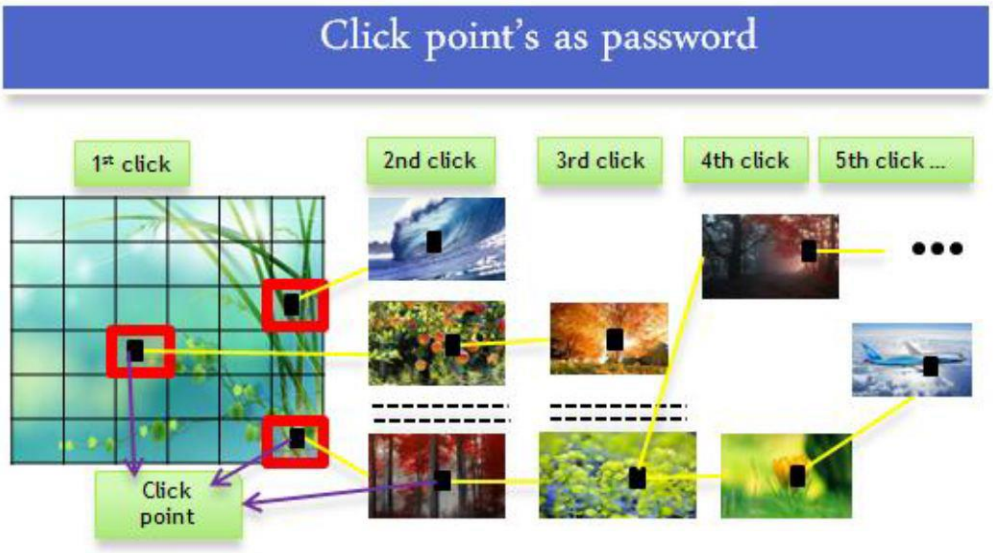
CONS: Hotspots is major security problem in which during password selection different users tend to choose similar click-points as part of their passwords. Attackers can gain knowledge of these hotspots by building dictionary attack and more successfully guess PassPoints passwords .

(d) CUED CLICK POINT(CCP):

Cued Click Points [7] was designed to reduce pattern based attack and the usefulness of hotspots for attackers. Rather than clicking five click-points on one image, CCP requires one click-point on five different images in proper sequence. The next image to be displayed is based on the location of the click-point entered previously, creating a path through an image set. Users select their images only to the extent that their click-point determines the next image. Creating a new password with different click-points results in a different image sequence.

PROS: Pattern-based attacks seem ineffective in CCP.

Users need not Remember the order of the click-points, as system presents only one image at a time. To protect against incremental guessing attacks explicit indication of authentication failure is only provided after the final click-point,.



Fig(9)Cued Click Point

CONS: Although attackers need to perform more work to exploit hotspots, still hotspots remain a problem for CCP .

(f) Persuasive Cued Click Points (PCCP):

For creating Persuasive Cued Click Points persuasive feature is added to CCP. PCCP [9] encourages users to select less predictable passwords. Viewport & shuffle terms are used for password creation and they are visible only during password creation.. Users requires to select a click-point within the highlighted viewport and is not allowed to click outside of the viewport unless shuffle button is not presses to randomly reposition the viewport .During password creation pressing shuffle number of times slows the process of creating password.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (15-25), Month: July - September 2015, Available at: www.researchpublish.com

Fig(10).Persuasive Cued Click Point

PROS: Guessing password becomes difficult for hacker. Pattern based attacks not possible due to large number of images, and click points.

CONS: Hotspot still remains an issue for PCCP.

III. SECURITY AND ATTACKS

In current graphical authentication systems attacks[10] can be divided Into 7 types which are brute force attack, dictionary attack, guessing, shoulder surfing, phishing, social engineering attack, and malware.

Table (2)Usability and security of Recognition Based System

Recognition Based Graphical Password Usability	Usability	Attacks
JANSEN ET AL	Theme based, Grid based, Easy and fun to use, Meaningfulness.	Brute Force, Guessing, Shoulder Surfing
Passface	Human Faces, Grid based, Easy and fun to use, User assign Image, Input Reliability and accuracy.	Brute Force, Guessing, Shoulder Surfing, Dictionary
Sobrado and Birget	Icon based, Easy and fun to use, Large Password Space	Brute Force, Guessing
DHAMIJA AND PERRIG AL	Abstract Image, Grid based, Easy and fun to use.	Brute Force, Guessing, Shoulder Surfing

The following subsections provide a brief introduction to the attacks:

A. Brute force attack:

Brute force attack also known as exhaustive-search attack, as it involves systematically searching all elements in a search space until the correct element is found. To overcome brute force attack effectively, a sufficiently large theoretical password space is necessary.

B. Dictionary attack:

Dictionary attack is a kind of brute-force attack where only passwords which are most likely to succeed are searched. Those passwords are derived from an exhaustive list named dictionary, typically consisting of all passwords with higher probability of being remembered easily, ordered from most to least probable.

C. Guessing:

Guessing attack is ubiquitous and every unauthorized user can attempt to guess the authorized user accounts and passwords to break into the system. With the development of Internet, personal information such as name, birthday, phone number and friends' names can be obtained much easier. And, users usually set their passwords associated with personal information to help recollection. Additionally, users may select passwords containing some other predictable character-istics, such as their favorite color. As such, attackers who know the user will have a higher probability of guessing the users also vulnerable to guessing attack as they are often predictable.

D. Shoulder surfing:

Shoulder surfing usually refers to using direct observation techniques, such as watching over a user's shoulder when the user enters a password or recording the user's input with some external device, to capture password . The presence of recording devices such as video camcorders and camera phones makes shoulder surfing easier to be done. Shoulder surfing is particularly effective in public places without user awareness.

E. Phishing:

Phishing is a way of trying to trick users into providing their login credentials and personal information, typically by sending an email containing a link to a fraudulent website and encouraging the user to follow the link .The phishing [8] website usually looks like the legitimate one, but the phishing website is designed only for an attacker to steal user information.

F. Social engineering attack:

"Social Engineering is a process in which attackers or hackers gain access to secure systems not by breaking into the system but by obtaining the required information like , username and password from a person. By using the natural human tendency the attacker makes users to trust to deceive thereby resulting out useful information.

G. Malware:

Malware, includes any unauthorized software designed to deny or disrupt, gather information that leads to loss of privacy, gain unauthorized access to system resources, and other abusive behavior. Examples include worms spyware, computer viruses, Trojan horses, and other malicious and unwanted software or program. Here we focus only on one category of malware which is intended to watch users' computers and record information about users without their knowledge, that is, key-loggers, mouse-loggers and screen scrapers. Keyloggers track the victim's input using the keyboard, mouse-loggers record the mouse actions and screen scrapers capture data from a display terminal's screen. In addition, a mouse-logger may also suffice if the attacker has additional information such as the position and size of the entry grid on the screen.

Table (3) Usability and security of Recognition Based System

Recall based Graphical Password	Usability	Attacks
DAS	Grid based, Drawing password, Large Password Space	Dictionary, guessing, Shoulder Surfing
Pass Go	Large Password Space, Theme based, Navigating Image.	Dictionary, guessing, Shoulder Surfing , Brute Force
Pass Point(PP)	Freedom Of choice, User assign Image , Large Password Space	Dictionary, guessing, Shoulder Surfing
Cued Click Point(CCP)	Freedom Of choice, User assign Image ,Large Password Space	Dictionary, guessing hotspot , Keylogger , Malware
Persuasive Cued Click Point(PCCP)	Large Password Space, System help user to assign password	Shoulder Surfing , hotspot guessing , Malware , Key Logger

IV. CONCLUSION

Thus we have studied in depth the classification of passwords along with Pros and Cons of each of them, focusing more on the Knowledge based authentication which is categorized into recall-based and Recognition based authentication. According to our survey we found that graphical password are more better alternative to textual password in terms of password space, memorability and different attacks like brute force, Pattern attack, Guessing attack, Social engineering attack but they are vulnerable to certain hotspot problems, shoulder surfing attack as well they lack somewhere in terms of usability. So future work concentrates on how Graphical Passwords can be made balanced in terms of both security and usability aspects in order to satisfy the users' requirements and needs.

REFERENCES

[1] Ankita R Karia, Dr. Archana B. Patankar," Image Based Authentication Using Persuasive Cued Click Points" Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 4, Issue 5(Version 6), May 2014, pp.179-185.

[2] Miss. Saraswati B. Sahu, Associate Prof. Angad Singh"Survey on Various Techniques of User Authentication and Graphical Password" International Journal of Computer Trends and Technology (IJCTT) – volume 16 number 3 – Oct 2014

[3] S. Chiasson, R. Biddle, and P. van Oorschot, "A Second Look at the Usability of Click-Based Graphical Passwords," Proc. ACM Symp. Usable Privacyand Security (SOUPS), July 2007.

[4] L. O"Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no. 12, pp. 2019-2020, Dec.2003.

[5] ROBERT BIDDLE, SONIA CHIASSON, and P. C. VAN OORSCHOT"Graphical Passwords: Learning from the First Twelve Years" ACM Computing Surveys, Vol. 44, No. 4, Article 19, Publication date: August 2012.

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

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

[8] R. Dhamija and J.D. Tygar, Phish and HIPs: Human Interactive Proofs to Detect Phishing Attacks. In:Baird, H.S., Lopresti, D.P. (eds.) HIP 2005. LNCS,vol. 3517, pp. 127–141. Springer, Heidelberg (2005).

[9] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot,"Influencing users towards better passwords: Persuasive cued click-points," in Proc. HCI, British Computer Society, Liverpool, U.K., 2008.

[10] .A. Salehi-Abari, J. Thorpe, and P. van Oorschot, "On Purely Automated Attacks and Click-Based Graphical Passwords," Proc.Ann. Computer Security Applications Conf. (ACSAC), 2008.