Graphical Password Authentication Schemes: Current Status and Key Issues

Harsh Kumar Sarohi[1], Farhat Ullah Khan[2]

[1] Department of Computer Science, Amity University, Noida, Uttar Pardesh, India

[2] Department of Computer Science, Amity University, Noida, Uttar Pardesh, India

Abstract

Authentication is one the most important security primitive. Password authentication is most widely used authentication mechanism. Users generally use characters as passwords but text-based passwords are difficult to remember and if they are easy to remember then they are vulnerable to various kinds of attacks and are predictable. To address these authentication problems, a new alternative authentication method have been proposed using pictures as passwords. It is supported by the fact that Human brain has remarkable ability to remember thousands of images with detail. Whereas it difficult to keep text in memory. In Graphical authentication user performs some events on pictures like clicking, dragging, moving mouse etc. In this paper, we conduct a comprehensive survey of the existing graphical authentication systems. We have classified these methods in to three main areas: Recognition based schemes, pure recall based schemes and cued recall based schemes. We will discuss their security and usability issues since efficiency of picture password is measured by these two factors.

Keywords: *Graphical password authentication, Picture Password, Graphical password Usability and Security, Graphical Password Schemes, Graphical Password Issues*.

1. Introduction

Authentication is the process of determining that the person requesting a resource is the one who he claims to be. Most of the authentication system these days uses a combination of username and password for authentication. The problem with the password is that you have to remember it and it should be kept secret. Each authentication system has their own rules and constraints like password length, password must contain alphabet, special characters etc. These passwords are mostly text-based passwords. Either users use passwords that are easy to remember like license plate number, pet name, phone number which are very much predictable or complex passwords which they tend to forget so either they use same password for different accounts or they write them down. Moreover, they are vulnerable to various attacks.

Text-based passwords suffered from security and usability issues. To overcome these shortcomings of alphanumeric passwords various graphical password schemes have been proposed. In graphical authentication systems a password consists of sequence of one or more images where user can input password with the help of mouse events like click, drag etc. Picture Superiority Effect Theory reveals that pictures can be recognized and recalled easily by human brain, enhancing the ability to remember. Since, images are used providing password space is quite large. Strong passwords can be produced that are resistant to guessing, dictionary attack, key-loggers, shoulder-surfing and social engineering. Graphical passwords have been used in authentication for mobile phones, ATM machines, E-transactions.

We can classify graphical password systems as

1) Recognition based authentication
2) Recall based authentication

2. 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.

2.1 Jensen et al. Method

Jensen et al. [1] 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. 1 Cats and dogs theme.

Fig. 2 sea and shore theme.

2.2 Passfaces Method

Real User Corporation developed a product called passfaces[2] 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. [3] Passfaces can be predictable as they are affected by race, gender and attractiveness.

Fig. 3 Passfaces Scheme.

2.3 Sobrado and Birget Method

Sobardo and Birget [4] 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.

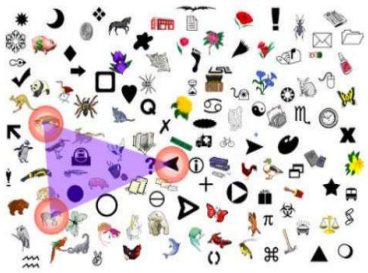

Fig. 4 convex hull shoulder surfing.

2.4 Hong et al. Method

Hong et al. [5] 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 recognising 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.

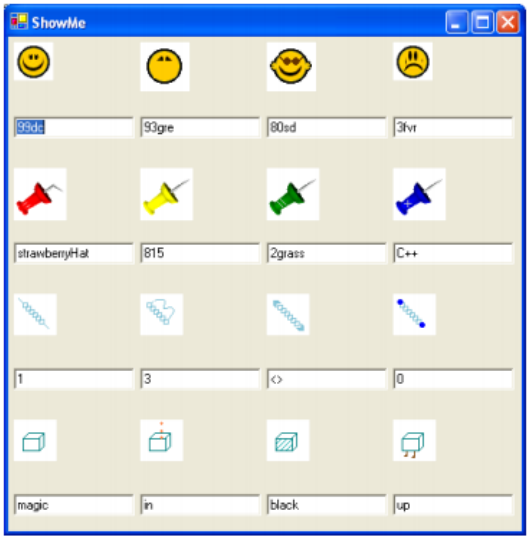

Fig. 5 Proposed beam former.

Fig. 7 Login Screen

2.5 Dhamiga and Perig Method

Dhamiga and Perrig[6] proposed a scheme called "Déjà vu" based on human ability to remember previously seen images. User has to select few images from a set of images. User has to perform same at login time. All abstract Images were generated using Andrej Bauer's Random Art.
They showed 90 % success rate using "Déjà vu" while only 70% using text-based password and pins

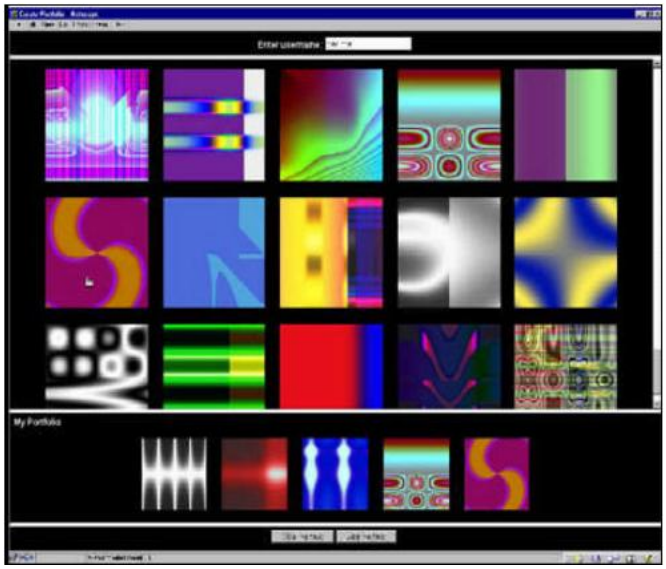

Fig. 6 Dhamiga and Perig Method

2.6 Akula and Devisetty's

User has to identify correct pass-image. It is similar to dhamiga and perrig. The only difference is that it store 20 byte hash code produced by SHA-1 hash function. It takes less memory but space occupied is still larger if compared to text-based password. They suggested using persistent storage for improvement.

3. Recall based Systems

3.1 Reproduce a Drawing

Jemryn et al. [7] proposed a technique called" Draw-a-secret (DAS)".In this scheme during registration 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.

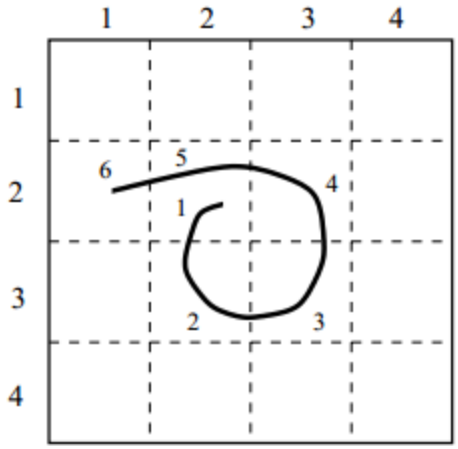

Fig. 8 Jermyn et al. DAS Scheme

3.2 Blonder Scheme

G.E blonder [8] 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.

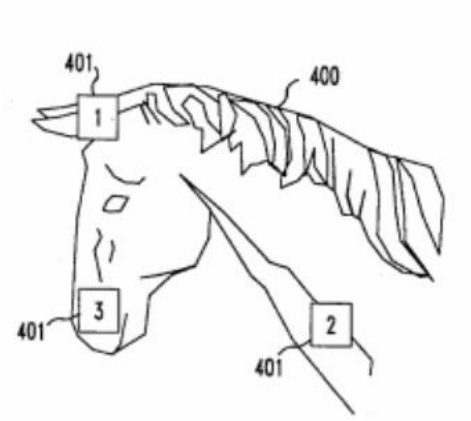

Fig. 10 Blonder Scheme

3.3 VisKey

SFR company [9] 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

3.4 v-Go

Passlogix [10] has proposed various schemes based on repeating a sequence of actions. In their v-Go scheme user has to select a background image e.g. kitchen, bathroom, bedroom and user can perform various actions with items present in image like clicking, dragging etc. Click on item is detected with the help of invisible boundaries on them. For example If kitchen is selected user can prepare meal by clicking and dragging cooking ingredients. The disadvantages of this technique included selecting weak passwords by users. Secondly, password space is small.

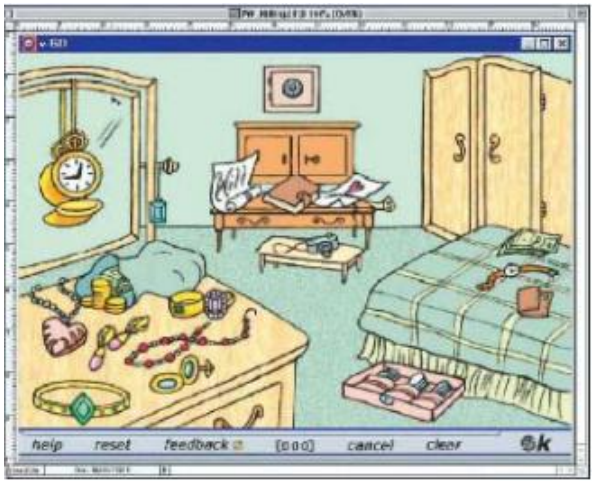

Fig. 11 v-Go

3.5 Pass-Point

Wiedenbeck et al. [11, 12] proposed a scheme in which user has to select a background. User can click arbitrarily on the image to register sequence of click points on image to be taken as password. When logging in, the user has to click on points as done during registration time. The click points are acceptable if they are within the predefined level of tolerance. This method has large password space. On doing Comparative study it was found that pass points are difficult to learn and it takes more time to input password as compared to text-based password.

Fig. 12 Pass Points Scheme

3.6 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.

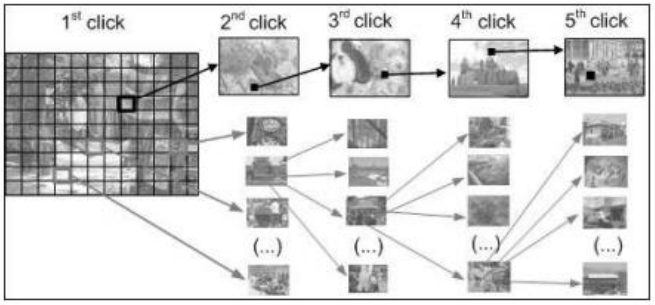

Fig. 13 Cued Click Points

4. Usability

There are many critical usability problems that hinder in the establishment of graphical authentication methods. Security and usability play important role in authentication process, but it is difficult to maintain balance between two as they are in conflict with each other. These problems need to be addressed. We have conducted a comparative study of usability features in various Graphical password schemes as shown in Table1

4. Security

We analyze the various possible threats in authentication.

4.1 Shoulder surfing attack

Passwords can be stolen by making observation on the user. Closed circuit hidden cameras can be placed for tracking the entry made into the system. This attack is possible on all available graphical schemes as well as on text based passwords.

4.2 Brute force attack

Text based passwords have password space of 94^N.It is difficult to do this attack on graphical passwords .We believe it is harder for this attack to succeed for graphical passwords. Recall based Password is more secure then recognition based techniques when it comes to brute force attack. Draw-A-Secret is resistant to this attack all other authentication techniques are vulnerable to this attack.

4.3 Guessing

It is almost impossible to get graphical password by phishing or using any other human interaction method.

4.4 Social Engineering

This attack practically impossible in graphical passwords as keyboard input is not involved so words in dictionary can't be used to crack the password.

4.5 Spyware attack

So far this attack is not possible on graphical passwords. Screen recording is possible. There are no such spywares till date. Text based passwords can be stolen using key loggers.

5. Conclusion

There has been growing interest in picture passwords; recently one of Microsoft's operating system windows 8 has used this for authentication .This paper throw light on various graphical authentication methods. We believe that main reason for using graphical password is they can be easily recalled. Furthermore, graphical passwords are more secure than text based passwords. During our analysis we found that it is very difficult to perform attacks on graphical passwords like brute force, Dictionary attack, and spyware. In our findings we can see that authentication process is slower in graphical password. Security and usability of graphical passwords are two main challenges for researchers.

Table 1: Usability features

Technique	Login Interface	Drawback
Jensen et al.	Select images based on a theme	Small password space
Passfaces	Select face from of grid of faces	Predictable
Sobrado and Birget	Select object from number of display	Difficulty in identifying objects from crowded display of objects
Hong et al.	login screen divided in to grids each grid containing a icon	Login Process time consuming
Dhamiga and Perrig	Identify correct pass images	Authentication process time consuming and larger load on server
Akula and Devisetty's.	Identify correct pass images	Authentication process time consuming
Draw a Secret	Redraw such that the drawing touches the registered sequence of coordinates	Difficulty in redrawing precisely
Blonder Scheme	Click within those tap regions and in a sequence.	If input precision is large password will be easy to crack, if small it will be difficult for the user to tap at exact points.
VisKey	select an image from the images stored in the device	User cannot click where he wants because of predetermined tap regions.
v-Go	Repeating a sequence of actions	Weak passwords, password space is small
Pass-Point	Make sequence of click points on image	passpoints are difficult to learn
Cued Click Point	make single click on multiple images	Hotspots still remain an issue

Acknowledgments

The authors would like to thank Amity School of Engineering and Technology (ASET) where the research was carried out.

References

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

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

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

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

[5] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware", In Proceedings of International conference on security and management, Las Vergas, NV, 2004.

[6] R. Dhamija and A. Perrig. "Déjà vu: A User Study Using Images for Authentication", In Proceedings of the USENIX Security Symposium, 2000.

[7] 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.

[8] G. Blonder, "Graphical Password", In Lucent Technologies, Inc., Murray Hill, NJ,United States Patent 5559961, 1996.

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

[10] Passlogix, http://www.passlogix.com, Accessed on February 2007.

[11] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication Using Graphical Passwords: Basic Results", In Human-Computer Interaction International (HCII 2005), Las Vegas, NV, 2005.

[12] S.Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., Memon, N., "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System", International Journal of Human-Computer Studies, 63, 2005, pp. 102-127.

Harsh Kumar Sarohi is pursuing M.Tech in Computer Science and Engineering from Amity School of Engineering & Technology at Amity University, Noida, Uttar Pardesh, India. He has done B.Tech from Shobhit University in 2011. He has worked as a Software developer. He has implemented research projects such as Content Based Image Retrieval using Color Classification; CBIR using perceptual hashing etc. His research interests include Image retrieval, Image Authentication, Image Processing.

Farhat Ullah Khan has done his M.Tech in Information Technology with specialization in Intelligent Systems, from Indian Institute of Information Technology Allahabad (IIITA) in the year 2010. He has served as software developer in an IT company. He has also done BCA and PGDCA. He has qualified Microsoft Certification (MCP) in ASP.Net using C#. He is a member of IEEE and IET UK. . Currently he is an Assistant Professor in Amity School of Engineering & Technology at Amity University, Noida, Uttar Pardesh, India. Professor Khan is contributing in the research areas like Intelligent Systems, Natural Language Processing; Machine learning and soft computing.