International Journal of Trend in Research and Development, Volume 2(5), ISSN 2394-9333
www.ijtrd.com

Graphical Password Authentication: Methods and Schemes

Geeta M. Rane,
Student (BE) of Computer Science and Engineering,
Shri Sant Gadge Baba College of Engineering & Technology, Bhusawal,
North Maharashtra University, Jalgaon, Maharashtra, India.

Abstract: Authentication is a method of defining whether somebody or something is. It is key element in security. For authentication generally textual passwords are used. Passwords are the most commonly used technique for recognizing operators in computer and communication organizations. Generally, passwords are sequences of letters and digits, i.e., they are alpha-numeric. Such passwords have the shortcoming of being tough to recall. The solution of this problem is Graphical passwords, which consist of specific actions that the user implements on an image. Such passwords are easier to recall, but are susceptible to shoulder surfing. Graphical passwords consist of choosing images or drawing symbols rather than entering textual characters. It has been recommended that graphical passwords are harder to predict or to be broken by brute force search. Similarly, the dictionary attacks are difficult. This paper presents a comprehensive study of graphical password authentication methods, and graphical password systems.

Keywords: Password, Graphical, Textual, Authentication, Brute Force, Shoulder Surfing, Dictionary Attack

I. INTRODUCTION

Alpha-numeric passwords were first presented in the 1960s as a result to security issues for first multiuser operating systems. As the name specifies, an alpha-numeric password is only a sequence of letters and digits. While nearly any string can select as a password, these passwords only over good security as long as they are complex enough so that they cannot be predicted. Normally used rules for alpha-numeric passwords are:

- The password must be at least 8 characters elongated.
- The password should not be easy to relate to the user (e.g., last name, birth date).
- The password must not be a word that can be set up in a dictionary or public directory.
- Preferably, the user should combine upper and lower case letters and digits.

When the mind is already flooded with hundreds of jobs, recalling these passwords is a redundant job. Shortcomings of alpha-numeric password is the dictionary attack, Brute force search, guessing. Since the trouble in recalling random sequences of characters, most users have a habit of to choosing a common word, or a name.

Graphical passwords consist of choosing images or drawing symbols rather than entering textual characters. It was first described by Greg Blonder in 1996. Human brain is capable of processing and storing large volumes of graphical information with easiness. While it is very tough to recall a string of fifty characters, humans are capable easily to recall faces of people, places we visited, and things. These graphical records characterize millions of bytes of facts and thus make available to big password spaces. Thus, graphical password schemes deliver a way of creating more human-friendly passwords while growing the level of security.

The benefits of graphical password are dictionary attacks are infeasible, moderately because of the huge password space, but primarily because nearby no pre-existing searchable dictionaries for graphical information. It is also hard to devise automated attacks. Possibly the major drawback for present graphical passwords is the shoulder surfing problem.

A. Graphical Password Authentication Methods

Existing authentication methods can be distributed into three main regions [2].

1. Token based authentication method
2. Biometric based authentication method
3. Knowledge based authentication method

1) Token based authentication

Token based techniques, such as important cards, bank cards and smart cards are extensively used. Lots of token-based authentication schemes also use knowledge based techniques to improve the security. For example, ATM cards are usually used collected with a PIN number.

2) Biometric based authentication

Biometric based techniques, such as fingerprints, iris photograph, or facial appreciation, are not until now broadly accepted. The main problem of this scheme is that such schemes can be costly, and the identification method can be slow and often untrustworthy. However, this type of system offers the uppermost level of security.

3) Knowledge based authentication

Knowledge based techniques are the furthermost broadly used authentication methods and contain both text-based and picture-based passwords. The picture-based methods can be further divided into two kinds: recognition-based and recall-based graphical techniques. Using recognition-based methods, a user is accessible with a set of images and permits the authentication by recognizing and isolating the images he or she selected through the registration phase. Using recall-based techniques, a user is requested to replicate something that he or she produced or selected previous during the registration phase.

B. Graphical Password Systems

The graphical password system can be classified as:

1. Recognitionbased authentication system
2. Recall based authentication system

1) Recognition based authentication system

In recognition based system, user is offered with a set of images and the user permits the authentication by recognizing and detecting the images he selected during the registration phase. Most important headings are to be column focused in a bold font without underline [1].

1.1 Jensen et al. Method

Jensen et al. [3] recommended picture password system for mobile PDAs in which user was requested to select a theme .Images of dimensions 40 x 40 were displayed in a 5 X 6 matrix on the foundation of selected theme, Operator have to pick images from the matrix with the help of stylus. A numerical order founded on image selection is recorded to form a password. At login period user has to identify same images in same order.

Main defect was that password space was small since, the numbers of images were restricted to 30.

Fig 1.1: Sea and Shore Theme

1.2 Passfaces Method

Real User Corporation developed a product called passfaces [4] it is maintained by the detail that human brain can rapidly recognize familiar faces. During registration user has to select 4 faces. The registration process is complete if the user appropriately identifies 4 passfaces two times successively. Through the login user is accessible with a login screen containing grid of faces. User has to select 4 faces: one face from each of 4 grids of 9 faces. The Passfaces can be expectable as they are affected by competition, gender and attractiveness.

Fig 1.2: Passfaces Scheme.

1.3 Sobrado and Birget Method

Sobrado and Birget [5] established a method to prevent shoulder surfing attack. During registration user was requested to select objects from no of displayed objects. At login time the user has to select objects nominated at registration time and then hit inside the convex hull formed by objects. To make password space larger 1000 items were used at login method. However, the display became crowded and it was difficult to find pass -objects.

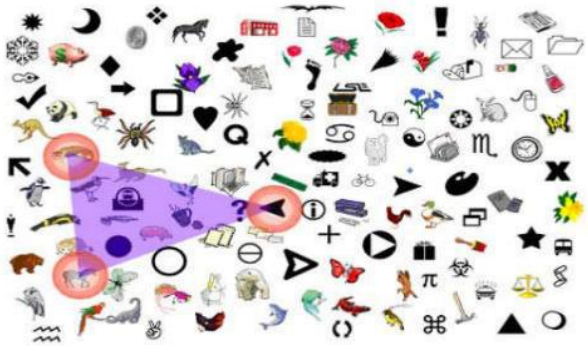

Fig 1.3: Convex hull shoulder surfing

1.4 Hong et al. Method

Hong et al. [6] proposed spyware resistant technique in which at registration time the user is offered with a login screen distributed in to grids each grid comprising of an icon. Each icon has number of differences (as shown in figure). User has to choose a pass-icons from the login screen .User has to enter a string consistent to each difference of pass -icons. At login period user is defied with

recognising the pass - icons from an n-grid login screen comprising no of icons. Each icon in grid is from dissimilarities of that icon. Once the icons has been properly identified user has to enter string conforming to the variation of particular pass -icon. Registration and login process in this scheme is time consuming.

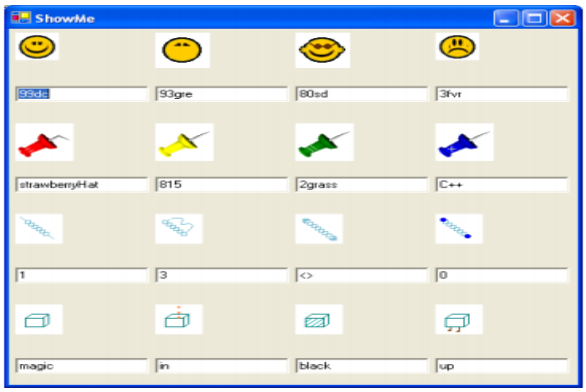

Fig 1.4: (a)

Fig 1.4: (b)

Fig 1.4: (a)Proposed beam former, (b) Login Screen

1.5 Dhamiga and Perrig Method

Dhamiga and Perrig [7] proposed a technique called "Déjà vu" based on human ability to remember formerly seen images. User has to choose few images from a s et of images. User has to execute same at login time. All abstract Images were created using Andrej Bauer's Random Art. They showed 90 % success proportion using "Déjà vu" scheme though only 70% by means of text-based password and tittles.

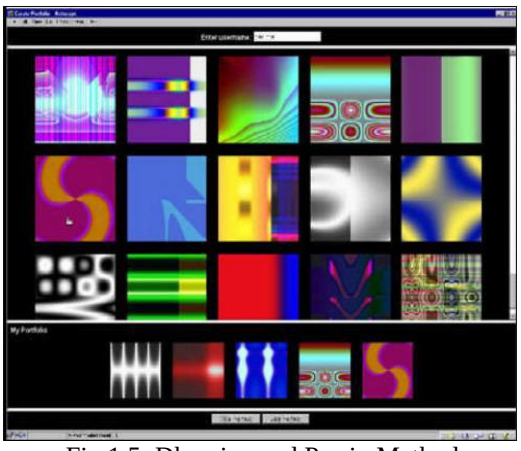

Fig 1.5: Dhamiga and Perrig Method

1.2 Recall based Authentication Systems

In recall based authentication technique, user is requested to replicate something that he formed or selected former during the registration stage.

2.1Draw-A-Secrete Methods

Jemryn et al. suggested a method known as" Draw-a-secret (DAS)" [8].In this system through registration user has to draw something on a GRID of size Y X Y. The coordinates (X, Y) of the grid were kept in the order of drawing. On the way to log in, user has to redraw such that the drawing touches the listed sequence of coordinates. This method lead to improved password space, concentrated traffic contents, since images were not moved over the network.

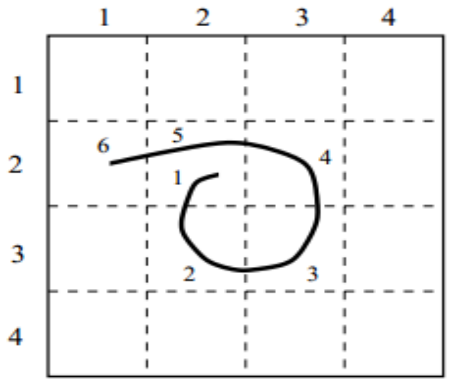

Fig 2.1: DAS Scheme

2.2 Blonder Scheme

G.E blonder [9] proposed a scheme in which an image is accessible to user with tap sections, for authentication user has to click inside those tap sections and in a order. The major disadvantages of this scheme was unforgettable password space besides, user cannot click where he wishes because of prearranged tap sections.

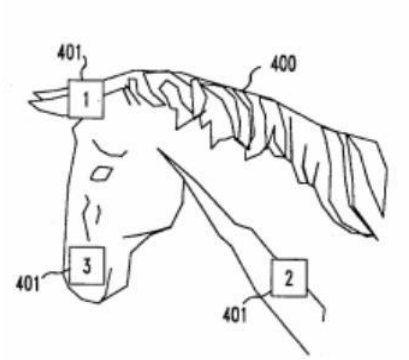

Fig 2.2: Blonder Scheme

2.3 v-Go

Passlogix [10] has suggested several schemes based on reiterating a sequence of actions. In the v-Go scheme user has to choose a background image e.g. kitchen, bedroom and user can implement several actions with objects exist in image like clicking, dragging etc. Click on object is identified with the help of invisible borders on them. For example if kitchen is selected user can make meal by clicking and dragging cooking ingredients. The drawbacks of this method included choosing weak passwords by users. Secondly, password space is minor.

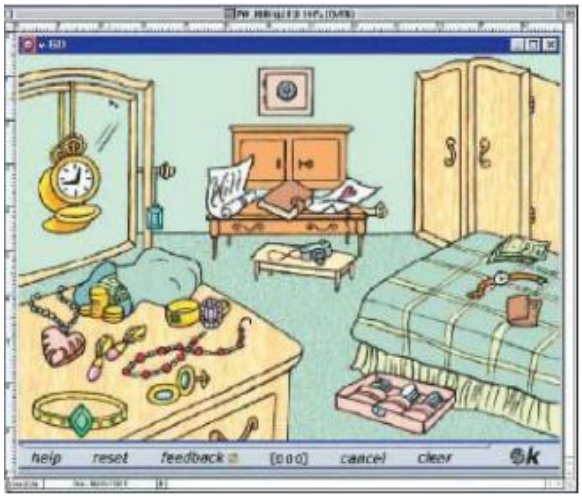

Fig 2.3: v-Go

2.4 Pass-Point

Wiedenbeck et al. [11] recommended a system in which operator has to choose a background. User can click randomly on the image to register order of click points on image to be occupied as password. When logging in, the operator has to click on points as done through registration time. The click points are tolerable if they are inside the predefined level of tolerance. This method has huge password space. On doing relative study it was set up that pass points are hard to learn and it takes additional time to input password as associated to text-based password.

Fig 2.4: Pass Points Scheme

CONCLUSION

The earlier decade has seen a rising interest in using graphical passwords as an alternative to the old text-based passwords. In this paper, I have conducted an inclusive study of present graphical password techniques. The current graphical password techniques can be categorized into two categories: recognition-based and recall-based techniques.

Though the main dispute for graphical passwords is that people are better at remembering graphical passwords than text-based passwords, the present user studies are very inadequate and there is not yet definite indication to support this dispute. My primary analysis recommends that it is harder to break graphical passwords using the traditional attack approaches such as brute force search, dictionary attack, or spyware.

Generally, the existing graphical password techniques are still undeveloped. Much more research and user studies are required for graphical password techniques to reach higher levels of maturity and helpfulness.

Acknowledgment

I feel great pleasure in submitting the paper on "Graphical Password Authentication: Methods and Schemes". I wish to express true sense of gratefulness in the direction of my H.O.D., Prof. D. D. Patil. I also wish to thank my teachers of the department who at very discrete step in preparation of this paper contribute her valuable guidance and help to solve every trouble that arose. Also, most likely I would like to express my sincere gratitude towards my family for always being there when I needed them the most.

References

[1] Harsh Kumar Sarohi, Farhat Ullah Khan, "Graphical Password Authentication Schemes: Current Status and Current Issues," IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 1, March 2013.

[2] "Graphical Passwords: A Survey" by Xiaoyuan Suo, Ying Zhu, G. Scott. Owen.

[3] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.
[4] Real User Corporation, Passfaces TM http://www.realuser.com, Accessed on January 2007.
[5] Sobrado, L and Birget, J. "Graphical Passwords", The Rutgers Scholar, An Electronic Bulletin of Undergraduate Research, Ruthgers University, New Jersey, Vol.4, 2004.
[6] D. Hong, S. M an, 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.
[7] R. Dhamija and A. Perrig. "Déjà vu: A User Study Using Images for Authentication", In Proceedings of the USENIX Security Symposium, 2000.
[8] 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.
[9] G. Blonder, "Graphical Password", In Lucent Technologies, Inc., M urray Hill, NJ, United States Patent 5559961, 1996.
[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.