ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

Review Paper

Graphical User Authentication Techniques

Shishir Anshuman*, **A M Aniket**

Computer Engineering Vishwakarma Institute of Information Technology, Maharashtra Pune 411048 India

Manuscript Info

Manuscript History:

Received: 15 September 2015
Final Accepted: 22 October 2015
Published Online: November 2015

Key words:

****Corresponding Author***

Shishir Anshuman

Abstract

As known, alphanumeric passwords are most often used for computer authentication, which requires a significant amount of human involvement. Users either create a short, simple and insecure passwords or long ones which are hard to remember. In this paper we evaluate a technique that can be used to replace the alphanumeric passwords for user authentication. The technique is commonly termed as the Graphical User Authentication. This method is attractive since people usually remember pictures better than words. Our survey comprehensively covers the study of the graphical authentication systems, the benefits as well as the drawbacks of the graphical systems. The conclusion includes the current scenario of the user authentication and its applications, and the failures of the graphical authentication proposals.

INTRODUCTION

A password is a form of secret authentication data that is used to control access to a resource. It is kept secret from those not allowed access, and those wishing to gain access are tested on whether or not they know the password and are granted or denied access accordingly [1]. User authentication is a fundamental component in most computer security contexts. It provides the basis for access control and user accountability [2]. Alphanumeric passwords being versatile and easy to implement are the most commonly used user authentication. But these methods are known to have security problems [3] and openly hated by the users [4]. Several techniques have been proposed to reduce the limitations of Alphanumerical password. One proposed solution is to use an easy to remember long phrases (passphrase) rather than a single word [5]. Another proposed solution is to use graphical passwords, in which graphics (images) are used instead of alphanumerical passwords [6]. It's a known fact that security experts focus more on security but less on usability and practical issues related to the deployment; usability experts tend to be optimistic about security. These and other factors have contributed to a long-standing lack of progress on how best to evaluate and compare authentication proposals intended for practical use [7].

Graphical passwords have been proposed as a possible alternative to text-based, motivated particularly by the fact that humans can remember pictures better than texts. Pictures are generally easier to be remembered or recognized than text, especially photos, which are even easier to be remembered than random pictures [8]. Graphical passwords were originally described by Blonder [9]. In his description, an image would appear on the screen, and the user would click on a few chosen regions of it. If the correct regions were clicked in, the user would be authenticated. In a graphical password system, a user needs to choose memorable image. The process of choosing memorable images depends on the nature of the process of image and the specific sequence of click locations. In order to support memorize ability, images should have meaningful content because meaning for arbitrary things is poor [1].

II. BENEFITS

Graphical Passwords were originally described as an appearance of a single image, after which the user would choose a few regions amongst it [10]. Authentication would be successful, if the correct regions were selected on the event of a click. Using graphical passwords, the user can create a visualization, which is meaningful enabling easy access for password retrieval. The use of this method suggests that Concrete, real world scenes will be more memorable, than abstract or jumbled images [11]. Studies have revealed that images are more memorable than words and sentences, as it enables easy recognition and recall process on being encountered. Efficiency is the one area where this system might lag behind alphanumeric password input, while the big question remains about the difference in that time lag.

The use of graphical passwords, brings about plenty of benefits to note. Benefits may mainly encompass categories such as usability, deployability and security [7]. The benefits mentioned have been narrowed down from a pre-existing set of points, which highlights the needs for this system.

A. Usability

- Memory capability- Users do not have to remember any secrets regarding the password. A proper visualized image can go a long way, to it being retained in the memory.
- Scalability - Such passwords can be effortlessly scalable, in a way, that it does not increase the burden on the user. Although, technical resources may remain the same, the scalability factor, can go a long way in helping the user, in manipulation of passwords.
- Easy to recognize – Figuring out the use of this system is easy, and once recognized, it can be easy to recall [7], Recognition involves, memorizing a set of imaged based on some standard pattern.
- Error reduction – Since a set of images are used, the process of error handling seems visibly easy, as errors are minimized.
- Efficient – The time taken for authentication is short, which makes the system more user friendly.

B. Deployability

- Accessibility – Users who need to use this system, can use it under any conditions, without the fear of prevention.
- Compatibility - The system is compatible with any kind of server [7] with no change required for the authentication process. Up to date standard softwares are the minimum requirement for compatibility.
- Cost – The total cost required to deploy the system, might be high at the initial phase, but the cost related to future add-ons is negligible.

C. Security

- Removal of Guessing – An attacker, in this case, has constraints with respecting to computing resources, and chances of a password hack, are fairly non-existent by using this system [7].
- Unauthorized attacks – It is comparatively more difficult to carry out third party attacks, against graphical passwords, as compared to text based passwords. This is due to the methodology involved in the attack programs, which have to be extremely accurate with respect to graphical passwords, with high accuracy to navigate and duplicate mouse motion of human input.
- Resilient to Phishing – Simulation of a user by an attacker, does not lead to collection of credentials that can be used to impersonate, the user with the actual verifier [7].

Vulnerability – It is less vulnerable to high profile attacks such as keyloggers on sensitive information. The attacks involve a lot of correlation, with application window and its size, which is hard to execute.

III.GRAPHICAL PASSWORDS METHODS

Few graphical password systems based on recognition and recall-based are discussed in this section. Graphical password techniques from 1994 till January 2009 shows that the techniques can be categorized into two groups as below:

A. *Recognition- based technique*

In this category, users will choose pictures, icons or symbols from a collection of images. In authentication process, the users need to recognize their registration choice among a set of candidates [1]. The research shows that 90% of users can remember their passwords after one or two month [12].

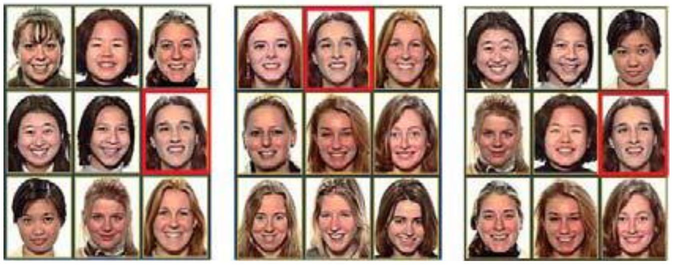
B. *Pure Recall-Based Technique*

In this category, users need to reproduce their passwords without being given any reminder, hints or gesture.

IV RECOGNITION BASED TECHNIQUE

A. PASSFACE

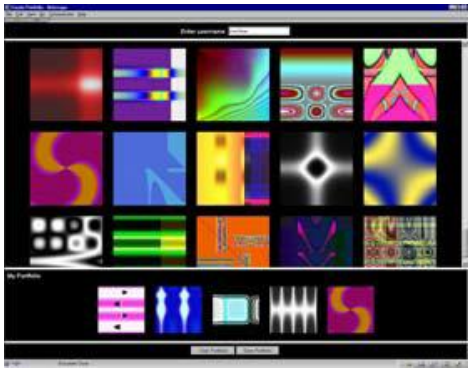
Passfaces algorithm, a commercial product of Real User Corporation requires a user to choose a face from a grid of image faces shown. To authenticate the user, an image grid of 9 human faces is shown to the user. The user has to choose an image of a human face from the grid which should be one of the 4 human face images that the user chose during registration. The user needs to choose all 4 human face images from the grid before authentication is complete [13] [14] [17].



B. Déjà vu

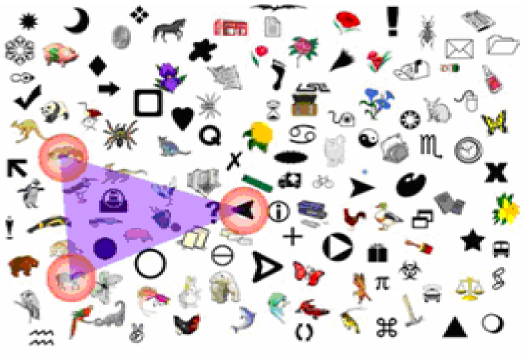
Dhamija and Perrig [15] in Year 2000 proposed an algorithm called Déjà vu. In this algorithm, users are required to select a specific number of pictures from a large image portfolio based on a hash visualization technique.

During an authentication session, the user is required to identify the selected images upon which the user is then authenticated. Dhamija and Perrig claimed that this algorithm offers a better security because it is almost impossible to write the authentication key due to the fact that abstract images cannot be easily described with words [16] [17].



C. TRIANGLE

Sobrado and Briget [18] proposed this algorithm to solve the shoulder surfing security problem. In this algorithm, the user needs to select the pass-images chosen during registration from a set of many displayed objects. The algorithm requires the user to click the inside of the convex hull which forms the pass-object. The author of this algorithm suggests that the displayed objects during the login process should be increased to 1000 objects to make the password space large enough and difficult to guess. This algorithm suggests that the user must find only 3 of the pass-objects among the displayed objects to form an invisible triangle shape to be authenticated. In practice, the number of objects must be randomly scattered on the screen and the objects must be different enough so that the user must be able to distinguish them [17].



D. MOVABLE FRAME

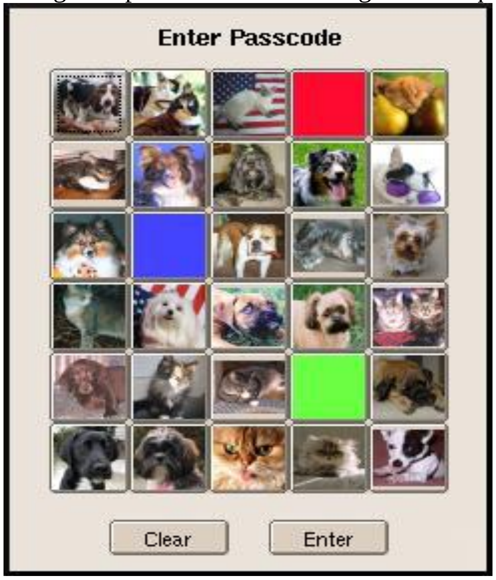
In this scheme, the user must also locate 3 of the pass-objects and move the frame until the pass-objects on the frame lines up with the other two pass-objects inside the frame [15]. A key difference between the "moving frame scheme" and the "triangle scheme" is that in the moving frame scheme, only 3 pass-objects are displayed at any given time and only one of them is placed in a movable frame [17].

E. INTERSECTION ALGORITHM

Sobrado and Briget [18] proposed in this algorithm that four pass-objects are located from the displayed objects and are used to form an invisible intersection point (Figure 7). The user has to click the inside of the convex hull of the object nearest to the intersection point to be authenticated [17].

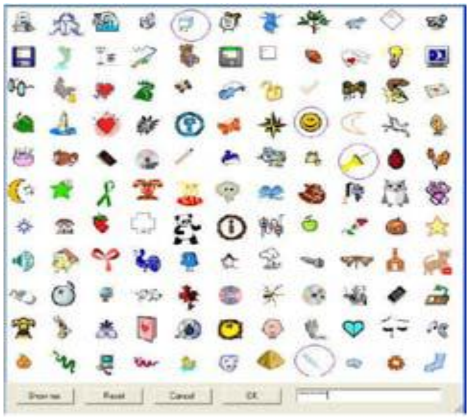
F. PICTURE PASSWORD

This algorithm was designed especially for handheld device like Personal Digital Assistant (PDA). During enrolment, a user selects a theme identifying the thumbnail photos to be applied and then registers a sequence of thumbnail images that are used as a future password. When the PDA is turn on, the user must enter the current enrolled image sequence for verification to gain access to the device. After a successful authentication, the user may change the password and selecting a new sequence or theme [1].



G. MAN ET AL.

This algorithm proposed as a new method for graphical password shoulder surfing resistant. In this algorithm all the pictures have assigned a unique code. During authentication the user is challenged with several scenes which contain several password objects and many decoy one. As there is a unique code for each password object, the user will enter the string of code for his password. It is very hard for shoulder surfer to crack this kind of password even if the whole authentication process is recorded [1].



H. STORY

In the Story scheme, proposed by Davis et al., [13], the user selects the password from a mixture of nine categories to make a story. The categories must be distinct and are derived from categories that depict our everyday life such as food, cars, pets, etc. The user must select from a given number of images, the selected images chosen during the registration period. Only when the sequences of images are correct, then the user is authenticated.

V. DRAWBACKS OF GRAPHICAL AUTHENTICATION SYSTEMS

- Although in less frequency, the password registration and further log in process, have known to be time consuming.
- Considering, the amount of methodology involved, and the sophisticated techniques, the amount of storage space is comparatively higher in comparison with text based passwords.
- Shoulder surfing is an issue still prominent in such systems. It involves, gathering of information, by spying over people's shoulders, leading to vulnerability in the system.

VI CONCLUSION

The use of graphical authentication has more or less replaced the text based password system, due to its vast security advantages, and the ramifications it has on the user's capability of remembering pictures more comprehensively. Firstly, this paper, gives a brief introduction of the system, and its advantages over conventional text based password authentication. Furthermore, several benefits have been enlisted which enlightens the use of this system. The use of this system in different recognition techniques, have been illustrated.

Lastly, it gives a brief view on the issues involved with the use of this technology.

VII ACKNOWLEDGMENT

We would wish to express our profound and sincere gratitude to Prof. Sachin Sakhare, Head of the Department, Department of Computer Engineering for his valuable support, guidance and his encouragement in the progress and successful study of this paper. As a team, we would like to dedicate this paper to our parents, who showed faith in us, helped us to understand the importance of knowledge and to make this paper a successful one.

REFERENCES

[1] Farnaz Towhidi and Maslin Masrom "A Survey on Recognition-Based Graphical User Authentication Algorithms", International Journal of Computer Science and Information Security, Vol. 6, No. 2, 2009

[2] William Stallings and Lawrie Brown. Computer Security: Principle and Practices. Pearson Education, 2008.

[3] R. Morris and K. Thompson, "Password security: a case history," Commun. ACM, vol. 22, no. 11, pp. 594–597, 1979.

[4] A. Adams and M. Sasse, "Users Are Not The Enemy," Commun. ACM, vol. 42, no. 12, pp. 41–46, 1999.

[5] Sigmund N. Porter. A password extension for improved human factors. Computers & Security, 1(1):54 – 56, 1982.

[6] Xiaoyuan Suo, Ying Zhu, and G. Scott Owen. Graphical passwords: A survey. In Proceedings of Annual Computer Security Applications Conference, pages
463–472, 2005.

[7] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot and Frank Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes", 2012 IEEE Symposium on Security and Privacy

[8] ISO-International Organization for standardization, http://www.iso.org/iso/catalogue_detail.htm?csnumber=1688

[9] Xiaoyuan Suo, Ying Zhu and G. Scott. Owen. "Graphical passwords: a survey," Proceedings of the 21st Annual Computer Security Applications. 2005, 463-472

[10] Blonder, G.E. (1996). Graphical Passwords. United States Patent 5559961.

[11] Susan Wiedenbeck, Jean-Camille Birget, Alex Brodskiy, Nasir Memon. "Authentication Using Graphical Passwords: Basic Results"

[12] 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.

[13] Omar Zakaria, Toomaj Zangooei, Mohd Afizi Mohd Shukran, "Graphical Password Authentication: Review and Analysis", AISS, Vol. 4, No. 15, pp. 25-32, 2012

[14] Lashkari, Arash Habibi, Azizah Abdul Manaf, Masrom Maslim, Salwani Mohd Daud. "Security Evaluation for Graphical Password", In Proceeding(s) of the Digital Information and Communication Technology and Its Applications, pp. 431-444. 2011.

[15] Rachna Dhamija, Adrian Perrig, "Déjà vu: A user study using images for authentication," In Proceeding(s) of the 9th USENIX Security Symposium, 2000.

[16] Mihajlov Martin, Borka Jerman-Blazic, "On designing usable and secure recognition-based graphical authentication mechanisms", Journal of Interacting with Computers, Elsevier, vol. 23 no. 6, pp. 582-593, 2011.

[17] Ejike Ekeke Kingsley Ugochukwu and Yusmadi Yah Jusoh, "A Review on the Graphical User Authentication Algorithm: Recognition-based and Recall-based"

[18] Sobrado L., Birget J, "Graphical Passwords, Rutgers University, Camden New Jersey. The Rutgers Scholar, An Electronic Bulletin of Undergraduate Research, vol. 4 (2002)

[19] Darren Davis, Fabian Monrose, Michael.K. Reiter, "On User Choice in Graphical Password Schemes," In Proceeding(s) of the 13th USENIX Security Symposium. San Diego, California, 2004