IJDCST @ Nov-Dec-2018, Issue- V-6, I-5, SW-12
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Pass Character Pair (PCP): A Graphical Password Mechanism for User Authentication

[1]Kameswara Rao.M, [2]Dr S.G.Santhi, [3]Dr Md.Ali Hussain,
[1]Research Scholar, Department of Computer Science and Engineering, Annamalai University
Email : mkraoau2016@gmail.com
[2]Assistant Professor, Department of Computer Science and Engineering, Annamalai University
[3]Professor, Department of Electronics and Computer Engineering, KLEF.

Abstract: User Authentication is one important aspect of computer security before allowing the user to perform certain tasks. Text based passwords are vulnerable to social engineering attacks. Graphical passwords have been employed to overcome such attacks. Graphical password employs graphical presentations such as icons, faces or custom images to create a password .Using images will decrease the tendency to choose insecure passwords. In this paper, we present a graphical password authentication mechanism which will be resistant to shoulder-surfing attacks and spyware attacks. Security analysis of the method's are also evaluated.

Keywords: Authentication, Graphical password, Security.

Introduction

Authentication determines whether a user should be allowed access to a particular system or resource. Conventional passwords are used widely for authentication, but they are known to have security and usability problems. Some drawbacks of conventional password appears like stolen the password, forgetting the password, weak password, etc .So a big necessity to have a strong authentication way is needed to secure all our application as possible. Researchers come out with advanced password called graphical password where they tried to improve the security and avoid the weakness of conventional password .Graphical password have been proposed as a possible alternative to text-based, motivated particularly by the fact that humans can remember pictures better than text. Psychological studies have shown that people can remember pictures better than text [1] and suggests that humans are better at recognizing visual information than recalling meaningless text-based strings.

Related Works

Graphical password schemes are categorized as Recognition Base Graphical Password schemes and Recall Base Graphical Password Schemes. In recognition-based techniques, a user is presented with a set of images and the user gets authenticated by recognizing and identifying the images he or she selected during the registration stage. In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. R.Dhamija et al [2] proposed a graphical authentication scheme where the user will be asked to identify a sequence of images that users select from a set of random pictures. Later, user will be required to identify the pre-selected images to be authenticated. Sobrado and Birget [3] developed a shoulder surfing resistant graphical password technique in which the system will display a number of pass-objects (pre-selected by user) among many other objects. To be authenticated, a user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects. In Man, et al [4] algorithm a user selects a number of pictures as pass-objects. Each pass-object has several variants with a unique code. During authentication, the user is presented with several scenes. Each scene contains several pass-objects (each in the form of a randomly chosen variant) and many decoy-objects. The user has 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 location of the pass-objects in reference to a pair of eyes. Jansen et al [5] proposed a graphical password mechanism for mobile devices. During enrollment stage, a user selects a theme (e.g. sea, cat, etc.) which consists of thumbnail photos and then registers a sequence of images as a password. During the authentication, the user must enter the registered images in the correct sequence. Takada and Koike [6] discuss a similar graphical password technique for mobile devices. This technique allows users to use their favorite image for authentication. The users first register their

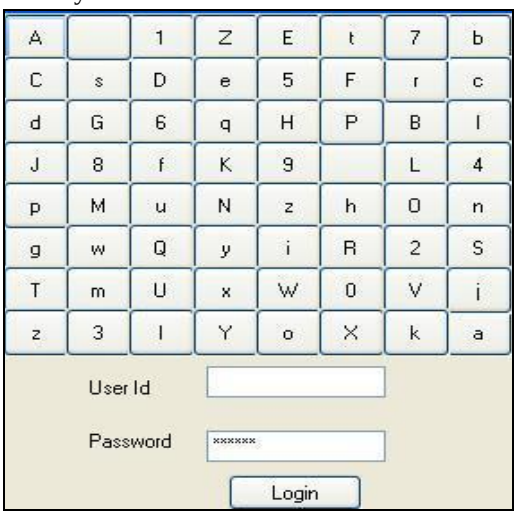
favorite images (pass-images) with the server. During authentication, a user has to go through several rounds of verification. At each round, the user either selects a pass-image among several decoy-images or chooses nothing if no pass-image is present. The program would authorize a user only if all verifications are successful. Real User Corporation developed Passface Algorithm [7] where the user will be asked to choose four images of human faces from a face database as their future password. In the authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces. Reproducing a drawing and Repeating a selection are the basic types of Recall based password techniques. Reproduce a Drawing group of authentication methods includes DAS (Draw-a-secret), Passdoodle method, Syukri method etc. Jermyn, et al [8] proposed Draw - a - Secret (DAS) Method, which allows user to draw their unique password. A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. Passdoodle Method developed by J.Goldberg et al [9] comprised of handwritten designs or text, usually drawn with a stylus onto a touch sensitive screen. Syukri ,et al [10] proposes a system where authentication is conducted by having user drawing their signature using mouse .The system will extract the signature area and either enlarge or scale-down signatures, rotates if needed, (also known as normalizing). The information will later be saved into the database. The verification stage first takes the user input, and does the normalization again, and then extracts the parameters of the signature for verification using geometric average means. In Repeat a Sequence of Actions group of authentication algorithms, a user is asked to repeat sequences of actions originally conducted by the user during the registration stage. Methods under this category include Blonder method, Passpoint method, Passlogix method etc. Blonder [11] designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas of those locations. PassPoint Method proposed by Wiedenbeck, et al [12] extended Blonder's idea by eliminating the predefined boundaries and allowing arbitrary images to be used. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of their chosen pixels and also in the correct sequence. Passlogix Method [13] was also based on blonder idea. In this method the users must click on various items in the image in the correct sequence in order to be authenticated. Invisible boundaries are defined for each item in order to detect whether an item is clicked by mouse. Many similar works are reported in [14, 15, 16, 17, 18].

Proposed Scheme

In this scheme, the available password icons set T is the set of all some printable characters(A-Z,a-z,0-9 ,2 spaces) , and |T | = 64 .Our scheme includes two main steps:

Step :1 The password creation step

In the first step, the user is asked to select a group of elements on the grid shown in the interface as the original password. In this example, we use g = 8×8 gird to show.Note that the size or the grid (g) can be different to meet the certain requirements and it could affect the security level of the scheme.



Step :2 Login Step

To login, the user must find all his/her original pass-characters in the login image and then make some clicks on the cells formed between the pass-characters or the user can input/type a textual characters chosen instead of clicking by mouse following the rules discussed below.

Click /Input Character rules

- If both pass characters appear on the same row of your grid, then input the character to the

immediate right of each pass character, wrapping around to the left side of the row if necessary. For example, using the gird, for the pass-characters "Z" and "7" the input characters would be "E" and "b" .Alternatively the user can click on any of the cells in the row that lie between the two pass-characters included .

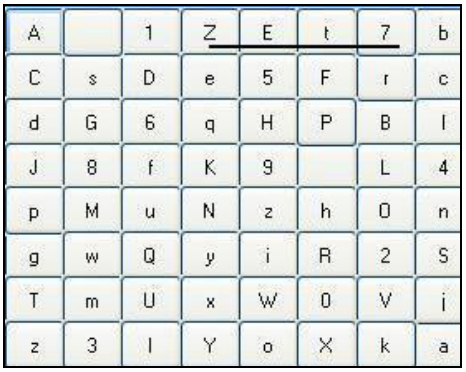
- If the pass characters appear on the same column of your grid, then input the characters immediately below, wrapping around to the top if necessary. For example using the gird, for the pass-characters "B" and "V" the input characters would be "L" and "k" .Alternatively the user can click on any of the cells in the column that lie between the two pass-characters included .
- If the pass-characters appear on different rows and columns, then input the characters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important - the first letter of the pair should be replaced first. For example using the gird, for the pass-characters "G" and "W" the input characters would be "H" and "m" .Alternatively the user can click on any of the cells in the row/column between the two pass-characters appear and the other pair of corners included .

- Special Case: If the two pass-characters are the same, they can be treated as to appear in same row or column. Hence in this case input any 2 characters that surround the pass character. For example using the gird, for the pass-characters "J" and "J" the input characters would be any of the two characters in { "D","G","8","M","p"}.Alternatively the user has to click on any of the cells that surround the pass-character.

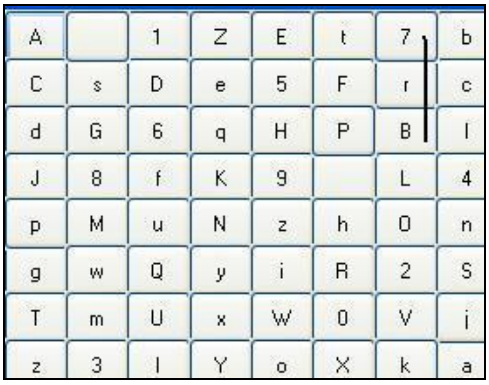
Login Process

To show the login process, let us follow an example we assume that the user Alice's original password is "Z7B3". The four combinations of password are considered as "Z7", "7B", "B3" and "3Z". The login procedure consists of the following four steps and is also shown below.

1)Alice finds her pass-characters "Z", "7" then clicks on any of the cells within the same row that lie between "Z" and "7" (included) or input a session pass-characters "E " and " b".



2) Alice finds her pass-characters "7", "B" , then clicks on any of the cells that lie within the same column between "7" and "B" (included) or input a session pass characters "r" and "L".



3) Alice finds her pass-characters "B", "3" then click on any of the cells in the row/column formed between the two pass-characters and the other pair of corners characters or input a session of characters "G" and "k" .

4)Alice finds her pass-characters "3", "Z" then clicks on any of the cells within the same row that lie between "3" and "Z" (included) or input a session pass-characters "I " and "3".

To resist the brute-force search, we introduce the "change image" technique. If a user fails in clicking the correct areas, or a user inputs wrong session password for I (e.g., I = 5) times, the client automatically changes the session login image.

Conclusion

In the present work, we have proposed a graphical authentication scheme that is shoulder-surfing and spyware resistant as the pass-characters are mapped into password regions that do not indicate a relation between the pass-characters and the input characters. The password space provided by the scheme is as much as that offered by conventional password systems. In
the proposed scheme, when the number of login attempts exceeds a certain threshold, say 3, the login screen is reset and no indication is given to the user if some of the characters are correctly input thereby deterring Brute force and Random click attacks. This work can be extended by an analysis of the probability of attacks and to eliminate the need for inputting session pass-characters in sequence for enhanced memorability.

References

[1] E. Shephard, "Recognition memory for words,sentences, and pictures",Journal of Verbal Learningand Verbal Behavior, 6, pp. 156–163, 1967.
[2] A. Jermyn, et al., "The design and analysis of graphicalpasswords", Proceedings of the 8th USENIX SecuritySymposium, August, Washington, D.C., USA, 1999.
[3] X. Suo,et al., "Graphicalpasswords: A survey.", Proceedings of 21st AnnualComputer Security Applications Conference., pp. 463–472, 2005.
[4] S. Chiasson, et al., "Graphical Password Authentication Using Cued ClickPoints", ESORICS, 24-27 September, Dresden,Germany, pp. 59–374, 2007.
[5] M. D. Hafiz, et al., "Towards Identifying Usability and SecurityFeatures of Graphical Password in Knowledge BasedAuthentication Technique",Proceedings of second AsiaInternational Conference on Modelling & Simulation,IEEE Computer Society, pp. 396–403, 2009.
[6] A. H. Lashkari, "A Survey On Usability AndSecurity Features In Graphical User AuthenticationAlgorithms",IJCSNS International Journal ofComputer Science and Network Security, 9, Korea,pp. 195–204, 2009.
[7] R. Biddle, et al.,"Graphical Passwords: Learning from the First Twelve Years",ACM Computing Survey, issue 44(4), 2011.
[8] R.Dhamija and A. Perrig, "Deja vu: A userstudy using images for authentication", Proceedings of9th USENIX Security Symposium, 2000.
[9] W. Jansen, "Authenticating Mobile Device UsersThroughImage Selection", Data Security, 2004.
[10] T. Takada and H. Koike, "Awase-E: Image-basedAuthentication for Mobile Phones using User"s FavoriteImages",Human-Computer Interaction with MobileDevices and Services, 2795, Springer-Verlag GmbH,pp. 347–351, 2003.
[11] Passfaces Corporation, "The science behindPassfaces", White paper, Available athttp://www.passfaces.com/enterprise/resources/whitepapers.htm, July 2009.

[12] J. Goldberg, "Doodling Our Way to Better Authentication",Proceedingsof Human Factors in Computing Systems (CHI),Minneapolis, Minnesota, USA.
[13] A. F. Syukri, et al., "A User Identification System Using Signature WrittenWith Mouse", Third Australasian Conference onInformation Security and Privacy (ACISP), Springer-Verlag Lecture Notes in Computer Science, pp. 403–441, 1998
[14] S. Wiedenbeck, et al.,"Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme, Proceedings of AVI, pp. 177–184, Venezia, Italy, ACM Press, 2006.
[15] B. Malek et al., "Novel shoulder-surfing resistant haptic-based graphical password". EuroHaptics '06, 2006.[21]M. Kumar,et al., "Reducing Shoulder-surfing byUsing Gaze-based Password Entry",in Symposium On Usable Privacy and Security (SOUPS). 2007: Pittsburgh, PA, USA, 2007.
[16] H.Zhaoand X. Li., "S3PAS:AScalable Shoulder-Surfing Resistant Textual-GraphicalPassword Authentication Scheme",AINAW '07Proceedings of the 21st International Conference onAdvanced Information Networking and ApplicationsWorkshops, vol. 2, pp. 467-472, 2007.
[17] A. Forget, et al., "Shoulder-Surfing Resistance with Eye-Gaze Entry inCued-Recall Graphical Passwords", Proceedings of CHI 2010, Atlanta, Georgia, USA, April 10 –15, 2010.
[18]. H. Gao, et al.,"A New Graphical Password Scheme Resistant to Shoulder-Surfing",International Conference onCyberworlds. 2010, IEEE: Singapore pp. 194 –199, 2010.