International Journal of Engineering & Technology, 7 (2.7) (2018) 984-987

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Spin Wheel Based Graphical Password Authentication Resistant to Peeping Attack

M. Kameswara Rao[1*], Dr. S.G. Santhi[2], Dr. Md.Ali Hussain[3]

[1,2] *Department of Computer Science Engineering, Annamalai University*
[3]*Professor, Department of Electronics and Computer Engineering, Koneru Lakshmaiah Education Foundation,*
**Email: mkraoau2016@gmail.com*

Abstract

Gadgets outfitted with touch screens rule the present versatile market in view of high adaptability and great convenience. Numerous security applications keep running on such gadgets. For user verification recalling or recognizing a secret word is testing errand in touch screen based gadgets. A graphical based secret key is a standout amongst the most encouraging and upcoming option for touch based devices. As per research, human brain can recall pictures more effectively than content. In this paper we introduce a novel spin wheel based authentication system targeting the touch screen based versatile and handheld gadgets. The user needs to rotate a set of spin wheels to get authenticated .Usability Study was directed to investigate the ease of use and security of the proposed authentication mechanism.

1. Introduction

In recent times, computer systems are very vital for its potential to keep and retrieve information in a more meaningful way. The most popular authentication manner for computer protection is the usage of alphanumeric password. However, this kind of authentication method come with few drawbacks. In recent years, many new strategies have been evolved with the aid of researchers to triumph over the dilemma of the password authentication, and one of the most famous approach is known as graphical password, which makes use of image as password rather than the alphanumeric string. Touch-Screen based gadgets have been broadly utilized in today's world. Individuals depend on Smartphone's to get to the Internet for messaging, texting, or information seeking. To ensure the applications and information put away on cell phone's composing text based passwords on a virtual console can be dull. Among numerous authentication schemes, password-based authentication are utilized on many touch based gadgets because of their lesser implementation and computational complexities.
However, numerous cryptanalysts located numerous vulnerabilities in textual content based schemes, e.g., dictionary attack, social engineering attack and so forth [1, 2]. Moreover, the tiny display screen length of the touch based gadgets imposes some extra constraints in text-based authentication schemes. An alternative is to investigate the utilization of graphical passwords for such touch based devices. Although, touch based gadgets come in specific sizes, most of the existing password-based totally authentication schemes are not screen size independent. Therefore, they fail to ensure the security of all sized smart gadgets [3, 4]. Hence, it remains a critical problem to research. In this paper, we tackle this problem through presenting a spin wheel based graphical authentication mechanism for touch screen based gadgets which give higher ease of use and better memorability. The paper is organized as follows. Section II gives a review of existing schemes that are related with our proposed scheme. In section III our proposed scheme is discussed in detail. Section IV provides usability and security study.

2. Related works

Several studies are conducted on the security issues and usability features of graphical passwords. All of them have centered on specific schemes or concrete attacks. Memory of passwords and viability of their information are two key components to be considered in an authentication mechanism. Graphical passwords have been expected to make passwords more exceptional and simpler for individuals to utilize and, accordingly, more secure. Many graphical secret schemes are projected in recent years. In line with the authentication fashion, the present day graphical passwords can be widely classified into three widespread categories:

1) Recall Based Schemes
2) Recognition Based Schemes
3) Cued Recall Schemes

In Recall based Schemes client is requested to replicate something (or) rehash an arrangement of activities that are made before amid enrolment process. Most usually utilized review based graphical watchword methods incorporate DAS (Draw A Secret)[5], Pass doodle[6], PASSMAP[7], Pass-Go Scheme[8] and so on. The Android OS utilizes a disentangled variation of the Pass-Go conspire called Pattern Lock [9] to expand ease of use and to adjust for the little screens found on ordinary gadgets running Android.
In Recognition based Schemes user is asked to select a certain number of images from a set of random pictures generated by a program. Later, the user should identify the preselected images in order to be authenticated. Examples include Passshapes [10], Jen-

sen et al. picture password [11], Sobardo and Birget's method [12], Hong et al. Method[13], Déjà vu[14]. Etc.

Cued Recall Schemes include Blonder plan [15], PassPoint plot [16], PassLogix [17], VisKey SFR Password [18], Cued Click Points (CCP) [19] and so on. Windows 8 Picture Passwords (W8PP), a cued recall plot is utilized as a part of Windows 8 [20].

3.Proposed Method

Our proposed scheme is a hybrid graphical password based authentication system, which means the password is both 'recall and recognize' based system. In our scheme we have two phases

1) Password Registration Phase
2) User authentication phase.

Password Registration Phase

The user is presented with a spin wheel that consists of 4 sub wheels with 36 different slots filled with numbers 1 to 36 in a random fashion. The four sub wheels of the interface can be rotated either in clock wise or anti-clock wise direction. During registration phase the user has to select one number from each sub wheel and arrange all the sub wheels in such a way that the four numbers selected by the user are in a row when pointed by any of the wheel axis.

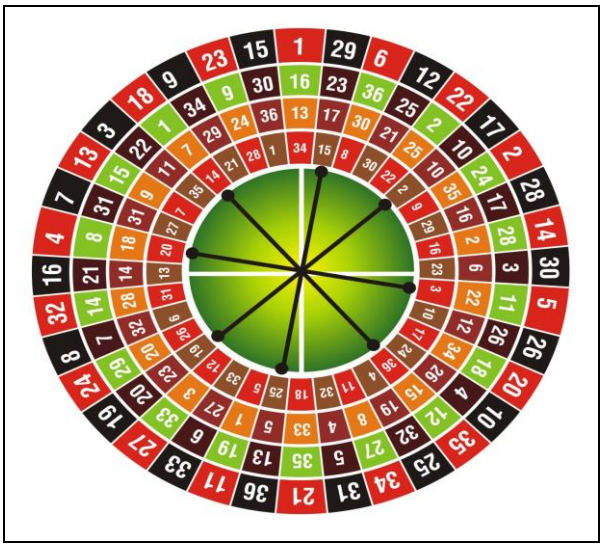

Fig 1: Login Interface of proposed scheme

The numbers selected by the user from four sub wheels along with their order become the user's password. For increasing the password space the user had an option to enter his own numbers in to the slots for selection of password.

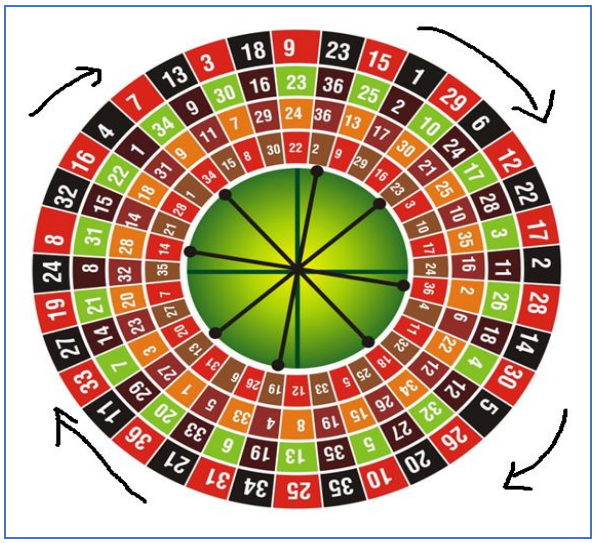

Fig 2: User Password Registration Phase

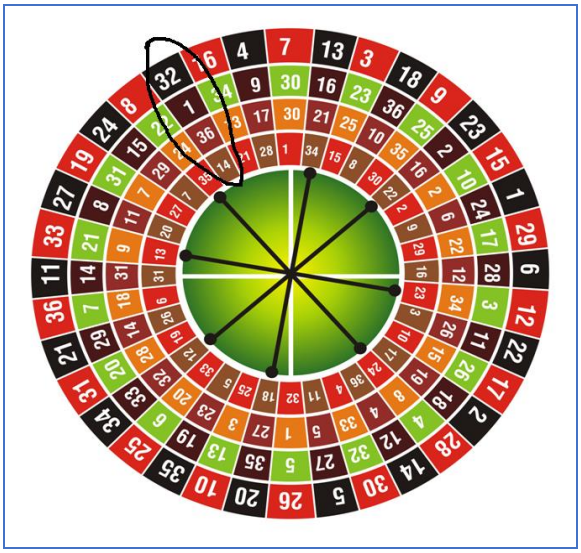

Fig 3: User Password Selection

During Password registration phase the user can rotate all the sub wheels in either clockwise or anti clockwise direction such that the selected numbers are in a row when pointed by any of the axis wheel.

For example let the user selects his password numbers as 32, 1, 36, and 14 in sub wheels as shown in fig 3. If the user forgets his password we need to have a backup which is provided in our system via security question. Here user is provided with a set of security questions and he has to pick one question and answer which is saved to the database of the system. This completes the password registration phase.

User Authentication Phase

For authenticating the user the screen the spin wheel interface with random shuffling of the number slots is displayed. The user simply has to rotate the sub wheels such that his password numbers are in same row when pointed by any of the axis of the wheel.

Fig 4: Login Screen for user Authentication

If the user forgets the password to unlock within three attempts user will be immediately asked a security question which is selected by the user himself in the phase I. If the security question is answered correctly then we repeat Phase I and create a new password.

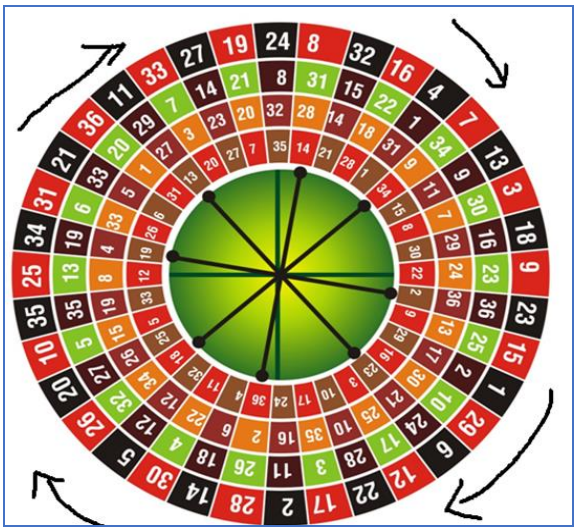

Fig 5: user rotating the sub wheels

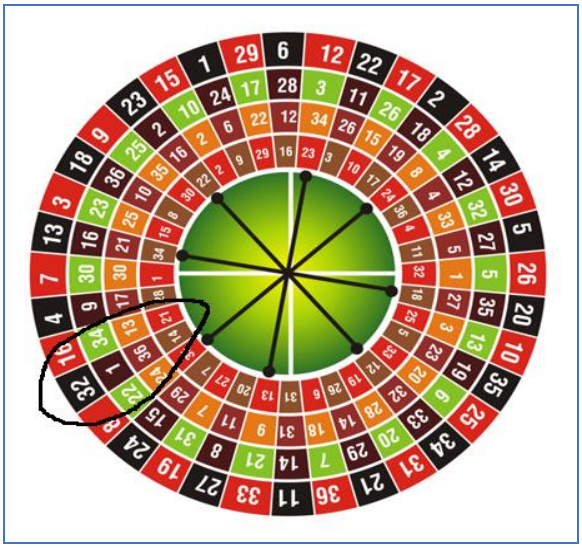

Fig 6: User arranging the password numbers

4. Usability and Security

Attacks on graphical passwords include dictionary attack, spyware attack, peeping attack and social engineering attack. The proposed method is resistant to dictionary, spyware and social engineering attacks because of its large password space. The user can also include the numbers of his choice in the slots which will increase the security of the proposed work. On the security viewpoint, the client inclination of choice of numbers in each sub wheel at each login exertion make the proposed method impervious to shoulder-surfing assaults.

The user can misguide the attacker who is performing the shoulder surfing attack by rotating the wheels in any direction of his choice, while keeping a look on his secret numbers. At each time the client logs in the numbers in the slots are shuffled which make the attack more difficult. If a client fails to login with in 3 attempts, the password has to be reset. Thus with a large password space and the rotation option with more axis pointing to , the shoulder surfer can be misguided.

A user study was conducted to check the effectiveness of the proposed approach in lowering peeping attack. We sent out e mail invites for volunteers to attempt out the proposed method. 46 people responded, 28 of them had been male, whilst 18 of them had been girl. All of them are mobile literate. A web based application is created and the participants are given instructions and the steps that they should use to be able to log in. The mean time recorded was just 23 seconds for selecting the password.

5. Conclusion

In the previous decade we have seen and came to realize that individuals are raising enthusiasm on comprehension and actualizing graphical passwords as a possibility for content based passwords. In this way, that individuals are preferred in retaining visual pictures over content. In this paper we proposed a spin wheel based authentication system which is easy to use even far a novice user and free from various attacks. The authentication mechanism proposed is resistant to all types of attacks.

The mechanism can be extended further by increasing the number of sub wheels along with user's choice to add both numbers and alphabet characters inside the slots. The work can be altered using pass objects or icons in place of the existing numbers.

References

[1] R. Biddle, S. Chiasson, and P. Van Oorschot. Graphical Passwords: Learning From the First Twelve Years. ACM Computing Surveys, 44(4):19:1{19:41 Sept. 2012.

[2] A. Jermyn, et al., "The design and analysis of graphical passwords", Proceedings of the 8th USENIX Security Symposium, August, Washington, D. C., USA, 1999.

[3] L. Sobrado and J. -C. Birget, "Graphical passwords, " The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[4] X. Suo, et al., "Graphical passwords: A survey. ", Proceedings of 21st Annual Computer Security Applications Conference., pp. 463–472, 2005.

[5] Jermyn Ian, A. Mayer, F. Monrose, M. K. Reiter and A. D. Rubin, "The design and analysis of graphical passwords", Proceedings of the Eighth USENIX Security Symposium. August 23-26 1999. USENIX Association 1– 14, 1999.

[6] C. Varenhorst, "Passdoodles: A lightweight authentication method', MIT Research Science Institute, July 2004

[7] A.. H. Lashkari, Samneh Farmand: A wide survey on Recall-Based Graphical User Authentication algorithm based on ISO and attack Patterns, IJCSIS Vol. 6, no. 3, 2009.
[8] Tao, H. and Adams, C. 2008. Pass-Go: A proposal to improve the usability of graphical passwords. International Journal of Network Security 7, 2, 273–292. [9] Tafasa. 2010. Patternlock. http://www. tafasa. com/patternlock. html.
[9] Weiss, R. and De Luca, A. 2008. PassShapes – utilizing stroke based authentication to increase password memorability. In NordiCHI. ACM, 383– 392.
[10] W. Jansen, "Authenticating Mobile Device Users Through Image Selection", Data Security, 2004.
[11] L. Sobrado and J.-C. Birget, "Graphical Passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.
[12] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme", In Proceedings of International conference on security and management. Las Vegas, NV, 2003.
[13] Déjà Vu: a user study using images for authentication by Rachna dhamija and Adrian perrig from SIMS/CS, Universtiy of California Berkeley.
[14] G. E. Blonder, "Graphical passwords, " in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996
[15] S. Wiedenbeck, et al., "PassPoints: Design and longitudinal evaluation of a graphical password system", International Journal of Human-Computer Studies, 63, pp. 102–127, 2006.
[16] M. Boroditsky. Passlogix password schemes. http://www. passlogix. com.
[17] Muhammad Daniel Hafiz, Abdul Hanan Abdullah, Norafida Ithnin, Hazinah K. Mammi; "Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique"; IEEE Explore, 2008.
[18] Chiasson, S. 2008. Usable authentication and click-based graphical passwords.
[19] Ph. D. thesis, School of Computer Science, Carleton University.
[20] http://windows. microsoft. com/en-in/windows-8/personalize-pc-tutorial.