ISSN: 2321-7782 (Online)
Volume 2, Issue 11, November 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Graphically Secured Password

Navgire Priyanka D[1]
Department of Computer Engineering
Vishwabharati Academy's College of Engineering
Ahmednagar, India

Prof. Jayapal PC[2]
Department of Computer Engineering
Vishwabharati Academy's College of Engineering
Ahmednagar, India

Kulkarni Swapnali V[3]
Department of Computer Engineering
Vishwabharati Academy's College of Engineering
Ahmednagar, India

Abstract: ***In Information security, user authentication has most essential areas. Most of the web application provides knowledge based authentication which includes alphanumeric passwords as well as graphical passwords. Graphical password plays an important role for user in security point of view. The existing system provides security for authentication in cloud by using graphical passwords which has limitation as username in text format. The proposed system provides better authentication by processing the username or user id using PCCP (Pervasive Cued Click Point) technique. The password is processed using CaRP (Captcha as gRaphical Password) technique.***

Keywords: Graphical passwords, PCCP, CaRP techniques, authentication, Security

I. INTRODUCTION

There are so many technical problems has been recognized especially when dealing with user authentication. Authentication method is of validating the identity of user/service or application. The use of authentication mechanisms can also prevent authorized users from accessing information that they are not authorized to view.

User authentication usually provided in the form of a password, is a type of security method that either allows or denies access to a system or resource depending on the ID presented. A password comprises of data authentication which is used to control access to resources. The security of a password is kept secret from unauthorized access while those who want to gain access use passwords for the system to be able to determine whether to endowment or deny them access accordingly.

In Ancient, the use of passwords can be traced back, when soldiers guarding a position would only exchange shifts only with a person who knew the password. Now-a-days passwords have been used to a wide range of applications such as operating any electronic devices to protect from thwarts like mobile phones, automated teller machines (ATM), and others.

The rest of paper is organized as follows: Section II presents Literature survey on graphical password schemes. Section III introduces PCCP and CaRP techniques. Section IV contains Security Analysis and section V concludes

II. LITERATURE SURVEY

Graphical password is an alternative solution to secure system rather than text based password. Reason behind is graphical pictures are more easily recalled than text. Graphical password schemes can be grouped into three general categories: recognition based, pure recall based, and cued recall based techniques [5].

Recognition Based Techniques:

In RBT , users have to select pictures, icons or symbols from a pool of images. During the authentication process, the users have to recognize their registration choice from a grid of image such as pass faces, story scheme, picture password and many more.

Firstly, a trial session starts with the user in order to have an exciting activity for the real login process. During the registration phase, images are in grid which was provided to user and have to select more than one.

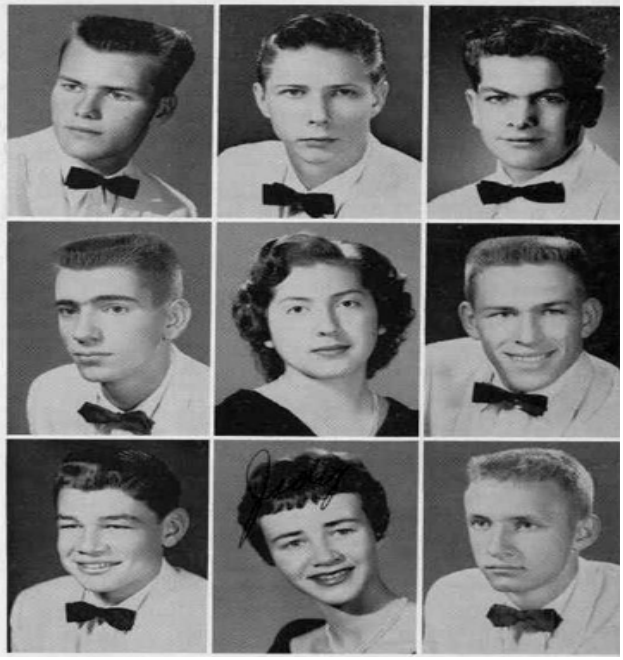

Fig 1: Pass faces

Pure Recall-based Techniques

In PRBT, without any clue or hint user generate his password. It follows many algorithms, which include passdoodle, DAS (draw-a-secret)and many more.

Fig 2: Passdoodle Scheme

Recognition inhibits the common use of the Passdoodle. Length and identifiable features of the doodle provides the boundaries of the system. A distinct number of computer differentiable doodles are possible. The doodle here is used as the only means of identification. A basic floor threshold of likeliness and similarity 11 for reasons of security, must be set, seeing as the system would refuse to authenticate a user as the user whose recorded doodle is most similar. This prevents guessing to authenticate a random user.

Cued Recall-based Techniques:

In CRBT, the image cues the user. For eg.to click a set of option a set of point on an image means hint and reminder help user to reproduce their passwords. It follows many algorithms, which include pass points, CCP(cued click points), PCCP(Persuasive cued click points).

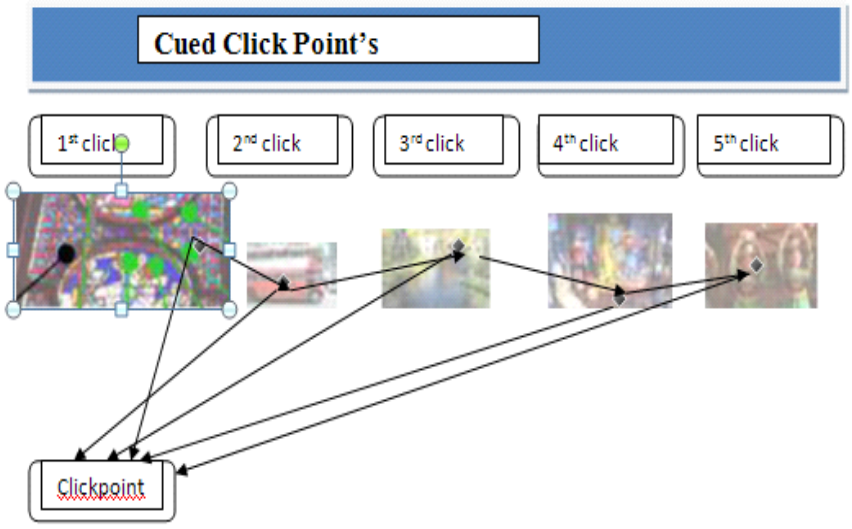

Fig 3: CCP

Cued Click-Points (CCP) is a click-based scheme where users select one click-point on each of 5 images presented in sequence, one at a time; this provides one-to-one cueing. The next image displayed is depend on previous image location(i.e where the user click on previous image). Users gets immediate feedback if they click on wrong location during login, seeing an image that they do not recognize. At this point they can restart password entry to correct the error. This feedback is not useful to an hacker not knowing sequence of images.

III. Proposed System

Persuasive Cued Click-Points (PCCP) [1][8] is a variation of CCP designed to persuade users to select more random passwords. It functions like CCP, but during password creation the image is blurred except for a small square viewport area randomly positioned on the image. Users select a click-point from within this viewport (see fig 4), or may press a \shuffle" button to randomly reposition the viewport until a suitable location is found. On subsequent logins, images are displayed in their normal format with no blur or viewport. Common perception that users choose the path-of-least-resistance here means selecting a click-point within the first or first few viewports. The design intent of the viewport is to pattern the distribution of click-points across multiple users, reducing hotspots and pattern formation.

PCCP:

Fig 4: PCCP

Different users might be select same images. Same images could be reused by two different users, highest probability of collision may be occurs. With the help of inclusion-exclusion principle will be minimized. PCCP reportedly removes major concerns related to common patterns and hotspots. PCCP use a grid-based discreatization algorithm [9] to find out whether

login click-points are within that tolerance area. In system-side storage for verification, these passwords can be hashed; additional information such as a grid identifier (for each click-point), however, is stored in a manner accessible to the system, to allow the system to use the appropriate grid to verify login attempts. It is unclear if attackers gaining access to the server-side storage can use these grid identifiers to their advantage.

CaRP :

Captcha is a standard Internet security technique to protect online email and other services from unauthorized access. It provide security against Man-in-the-Middle attacks, which can influence the communication between the user and the e-banking server.

Fig 5: Examples of captcha

Graphical password systems integrating Captcha technology, called as *CaRP (Captcha as gRaphical Passwords)*[6].

CaRPtechnique are click based graphical images. It can be classified into two categories:*recognition based* and a, *recognition-recall* .In *recognition based,* recognizing an image and using the recognized objects as cues to enter a password while in *recognition-recall* ,it combines recognition and cued-recall, and having advantage of both the recognition-based for remember easy for human brain and the cued-recall for large password space.

Flowchart of Proposed System:

Fig. 6 shows the registration phase, in which user have to select images from cloud and in Fig. 7 shows Log in phase

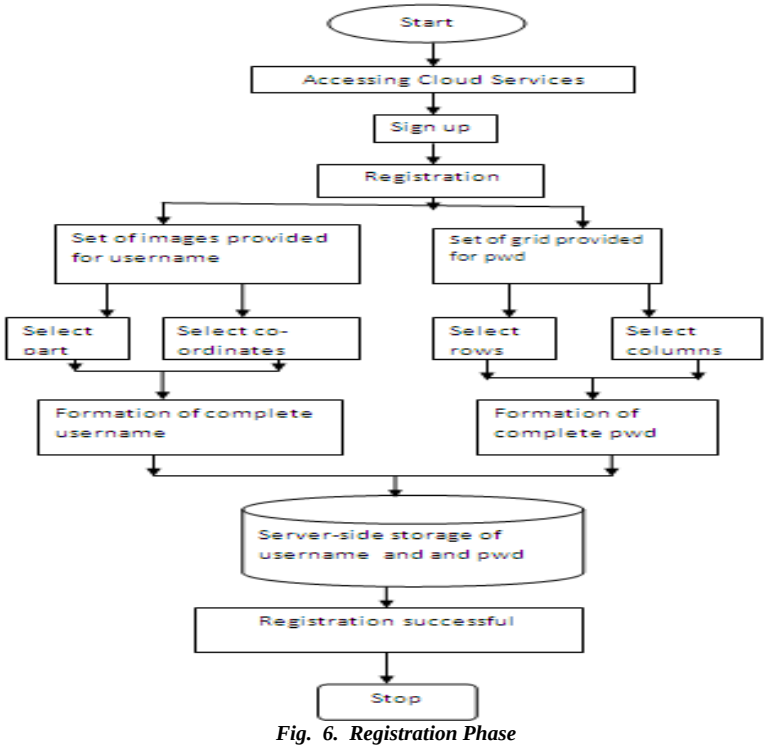

Fig. 6. Registration Phase

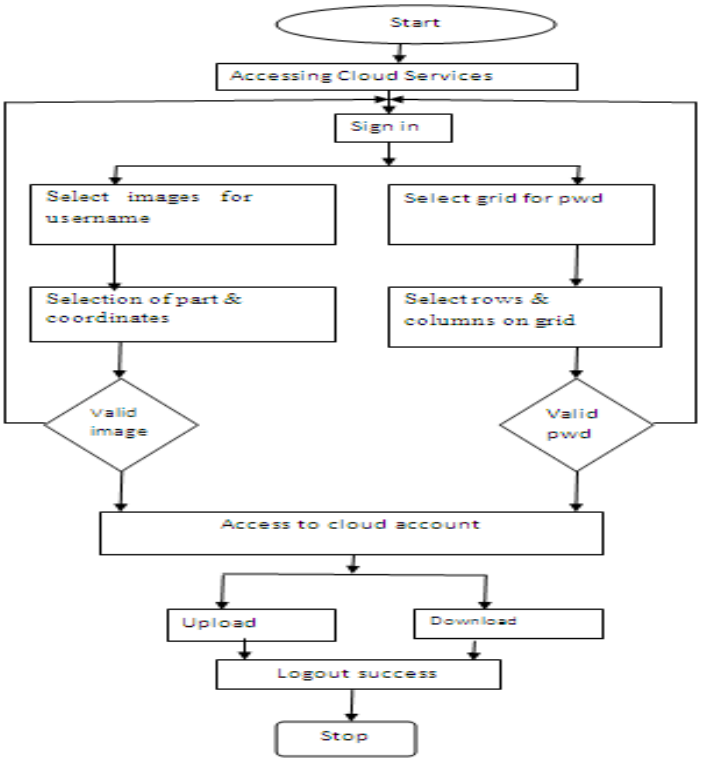

Fig. 7. Login Phase

IV. SECURITY

Brute force attack

In this attack, the attacker tries to check every possible value for a password until they succeed. Proposed reduces this attack, if no. of click partially known to attacker it is not sufficient because attackers doesn't known the length of the clicks.

Malware (Spyware attack)

Malware is a major anxiety for text and graphical passwords, since key logger, mouse logger, and screen scraper malware could send captured data remotely or otherwise make it available to an attacker.

Guessing Attacks

In successful guessing attacks, attackers are able to either exhaustively search through the entire theoretical password space, or predict higher probability passwords (i.e., user may create password as is birth date or name of any family member…etc) so as to obtain an acceptable success rate within a manageable number of guesses. Proposed reduces this attack, during registration ,many images we have to select that images contain viewport and user must have to click on that viewport only [1][8].

Shoulder Surfing

Like text password, Graphical password is also vulnerable to Shoulder-Surfing attack. Proposed reduces this attack, viewport is only visible at the time of registration phase.

Dictionary based attack

In this attack, an attacker tries each of the words in a dictionary as passwords to gain access to the system via some user's account. If the password chosen by the user was a word within the dictionary, this attack will be successful. This is a specific instance of the password brute forcing attack pattern. Proposed reduces this attack, no. of click contains co-ordinates of pixel only rather than text.

V. CONCLUSION

An important usability goal is that to help user's select better password with larger password space. Security goal in authentication system is that easy to remember but it is highly secure.

References

1. R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords:Learning from the first twelve years," ACM Comput. Surveys, vol. 44,no. 4, 2012.
2. R. Lin, S.-Y. Huang, G. B. Bell, and Y.-K. Lee, "A new CAPTCHA interface design for mobile devices," in Proc. 12th Austral. User Inter.Conf., 2011, pp. 3–8.
3. S. Li, S. A. H. Shah, M. A. U. Khan, S. A. Khayam, A.-R. Sadeghi,and R. Schmitz, "Breaking e-banking CAPTCHAs," in Proc. ACSAC,2010, pp. 1–10
4. S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Proc. ESORICS, 2007,pp. 359–374.
5. A Survey on Recognition-Based Graphical UserAuthentication Algorithms Farnaz Towhidi Centre for Advanced Software Engineering, University Technology Malaysia Kuala Lumpur, Malaysia
6. Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, "Captcha as Graphical Passwords- A New Security Primitive Based on Hard AI Problems" 2014
7. Xiaoyuan Suo Ying Zhu and G. Scott. Owen ―Graphical Passwords : A Survey.
8. Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle and PaulC. Van ―Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge- Based Authentication Mechanism, IEEE Transactions on Dependabale and Secure Computing Vol. 9 No. 2 March / April 2012.
9. S. Chiasson, J. Srinivasan, R. Biddle, and P.C. van Oorschot "Centered Discretization with Application to Graphical Passwords," Proc. USENIX Workshop Usability, Psychology, and Security (UPSEC), Apr.2008.

