Novateur Publication's
International Journal of Innovation in Engineering, Research and Technology [IJIERT]
ICITDCEME'15 Conference Proceedings
ISSN No - 2394-3696

AUTHENTICATION SCHEME USING PCCP AND GBAS TECHNIQUES

Priyanka Navgire
Department of Computer Engineering, PUNE University / VACOE, Ahmednagar, India

Mandar Kshirsagar
Department of Computer Engineering, PUNE University / VACOE, Ahmednagar, India

Namrata Kale
Department of Computer Engineering, PUNE University / VACOE, Ahmednagar, India

ABSTRACT
In Information security or in computer security, user authentication has most important or essential areas. Most of the web application offers knowledge based authentication which contains alphanumeric passwords as well as graphical passwords. Graphical password plays an important part for user in security point of view. Existing system has security for authentication in cloud by using graphical passwords which has some limitation as username in text format. Proposed system, provided better authentication to the username or user-id by using PCCP (Pervasive Cued Click Point) technique as well as password by using GBAS(Grid Based Authentication) technique.

INTRODUCTION
There are so many technical problems found especially when dealing with user authentication. Authentication method determines or 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 only, which is a type of security method that either allows or denies access to a system or resource depending on the ID presented. A password involves 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.
The rest of paper is organized as follows: Section II presents Background and Related work. Section III introduces Implementation. Section IV contains Usability and Security Analysis and section V concludes.

BACKGROUND AND RELATED WORK
Graphical password schemes can be grouped into three general categories based on the type of cognitive activity required to remember the password: recognition, recall, and cued recall. Recognition is the easiest for human memory whereas pure recall is most difficult since the information must be accessed from memory with no triggers. Cued recall falls somewhere between these two as it offers a cue which should establish context and trigger the stored memory. Among existing graphical passwords, CCP most closely resembles aspects of Pass faces [1], Story[1], and Pass Points [1]. Therefore these graphical password schemes are presented in more detail.
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.

IMPLEMENTATION

PCCP:
Persuasive Cued Click-Points (PCCP)[4] is a variation of CCP designed to persuade users to select more random co-ordinates for username. It is enhancements of CCP by adding some techniques.
Different or other 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 associated to common patterns and hotspots. PCCP use a grid-based discreatization algorithm to find out whether login click-points are within that tolerance area.

GBAS:

Grid Based Authentication Scheme is a some part of recognition-based CaRP[5](Captcha as a graphical password). In this scheme user has to select rows and columns to type their password.
In implementation, there are four phases:

1. Preprocessing phase
2. Registration phase
3. Login phase
4. Verification phase

PREPROCESSING PHASE: To achieve system involvement for click point's selection in login phase user has to follow the following steps:

- Image divided into blocks:2D images in the process of username creation. Images generally represented in X-Y co-ordinates.

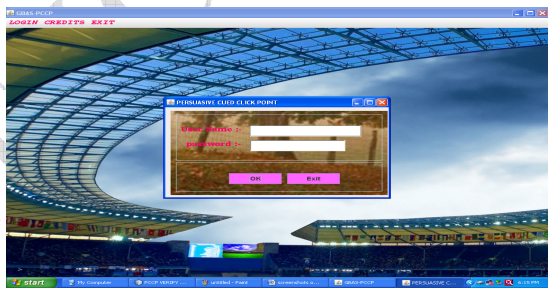
REGISTRATION PHASE: In this phase user have to create username by using images. User must be click only on activation portion only which he selected from blocks. In order to create username. Username is in co-ordinates only.

- Select/Activate only one block to select points: as shown in fig

Fig: Activation of Block

- For password, user has to type password in this phase. Finally these results (username, images, and password) stored in database.

LOGIN PHASE: In this phase, user has to click on images and internal processor check whether username is valid or not. For password, system provides grid based scheme to create password which was type at the time of registration phase. As shown in fig.



VERIFICATION PHASE: This phase was done by system administrator only. System check whether user is authorized or not.

USABILITY AND SECURITY
USABILITY

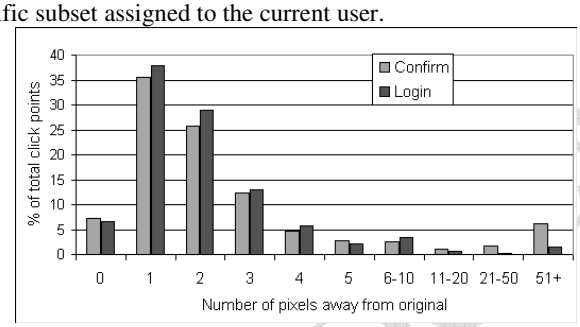
Participants used the reset/back button as per they saw an incorrect click and realized they were on the wrong path. A few times, participants restarted even when they saw the correct image because they had forgotten the image. Failed login attempts (where users pressed the login button and were explicitly told that their user-id/password was incorrect) occurred only when users clicked on the wrong point for the last image since they did not receive any implicit feedback for that click-point. Participants said that confirming the user-id helped them to remember it. Once they had successfully confirmed the password, logging on even after the distraction task was relatively easy. Refer table 1

Table 1. Total Number Of Restarts, Success Rates Of Create, Confirm And Login Phases.

	Create	Confirm	Login
Total no. of restarts	7	101	14
Success Rates	98%	83%	96%

SECURITY

Hotspots are specific areas in the image that have higher chances of being selected by users as part of their user-id. If attackers can accurately guess the hotspots in an image, then a dictionary of passwords containing groupings of these hotspots can be erected. Hotspots are known to be difficult for Cued Click Points; advance analysis is needed to determine whether insurances such as carefully selecting images can minimize this threat. A key advantage of PCCP over Cued Click-Points is that attackers need to analyses hotspots on a large set of images rather than only one image since they do not know the order of images used for a given password. Secondly, using different subsets of images for different users means that an attacker must somehow gather information about the specific subset assigned to the current user.



Four participants completed all their trials without any restarts, i.e., they made no errors during the entire session. The success rates were high for all phases, as shown in Table 1. Success rates were calculated as the number of trials completed without errors or restarts over the total number of trials.

CONCLUSION

New grid based technique reduces the vulnerabilities which was occurred in existing. User-id is in co-ordinates i.e, in graphical images so it is helpful to remember for user. By using PCCP technique we can provide security for user-id also, which was not provided in existing.
It can balanced both security as well as usability.

REFERENCES

[1] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using Cued Click Points," in European Symposium On Research In Computer Security (ESORICS), LNCS 4734, September 2007, pp. 359–374.
[2] Shraddha, Leena,Prathmeyy, Nilesh"Graphical Password Authentication for cloud securing scheme" IEEE 2014.
[3] XiaoyuanSuo Ying Zhu and G. Scott. Owen ―Graphical Passwords: A Survey.
[4] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle an 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
[5] 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
[6] 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.