ISSN NO. 2456-3129

International Journal of Engineering, Pure and Applied Sciences,
Vol. 3, No. 1, March- 2018

Random Positioning of Cued Click Point Based Graphical Password for User Authentication

Krishan Gupta[1], Shubham Sinha[2], Deepanshu Jain[3]

Computer Science Department, Bharti Vidyapeeth's College of Engineering, G. G. S Indraprastha University, New Delhi[1,2,3]
Email: krishanc3@gmail.com

Abstract-User authentication is an important factor for providing security. For the authentication process, passwords are used most frequently. The password provides a security mechanism for authentication and prevents an intruder from gaining access to the system resources. Alphanumeric passwords are most widely used in the authentication mechanism. But such passwords are vulnerable to remembrance and attacks. Graphical passwords are introduced to make the authentication system a lot easier. The graphical passwords are easy to use, remember and therefore, more secure. Here, instead of typing alphanumeric characters, a user has to click on image, cells or grids. To text passwords graphic based passwords are a suitable alternative, where users click on images/grids to authenticate themselves. For a sequence of images, users may have to click on a cell or coordinate point per image. The next image is determined based on the previous click-point and shown to user. This has been proven by experiments and researches that the humans have a natural inclination to remember images more easily than text.

Keywords- security, password, Alphanumeric, characters

1. INTRODUCTION

User authentication is the most important component in online security as well as authorization. It provides the valid user access
to the system resources. Many graphical models as traditional textual alternatives have been devised. Experiences over time plus plenty of researches have shown that text-based passwords are cumilated with both usability and security problems that make them less desirable solutions. To overcome these drawbacks and improve security, new scheme is developed which uses images, click points etc. as a user authentication tool. Picture cells and other grid oriented password model techniques are developed as an alternative.
Here graphics mean pictures in broad sense. Images are easier to recall and recognize than
text. To make a good authentication system, usability and security should be given equal importance. Strong passwords are resistant to dictionary attack, guessing, key-loggers, social engineering, shoulder-surfing, etc. Graphical passwords are currently used in authentication for mobile phones The following section briefly describes the need of Picture Password, Cued Click Points, Password Authentication using Picture Grids, how to improve security in Picture Password System and Security. Finally we provide the discussion of results.

2. PROBLEMS IN TEXT PASSWORDS

Alphanumeric passwords are often insecure. This in security arises mainly because of difficulty in handling alphanumeric passwords due to long-term memory (LTM) limitations. Users face difficulty in remembering system generated complex, pseudo-random passwords over time. Therefore, users often create memorable passwords which are easy for attackers to guess and thereby possesses a threat to security. An ideal authentication system should encourage providing strong passwords without hampering usability and memorability. If strong, then Alphanumeric passwords don't have meaning and can only be habitually memorized or by a weak way of remembering. Also it's common that users ignore system recommendations, instead use it simple passwords that are easier to predict using dictionary attacks or based on the knowledge of the user.

3. GRAPHICAL PASSWORD AUTHENTICATION TECHNIQUES

Graphical password techniques are classified into 2 categories, i.e., recognition-based and recall-based techniques, also Cued recall based technique, but then cued recall are gaining more popularity and thus shall be discussed.

4. CUED-RECALL BASED TECHNIQUE

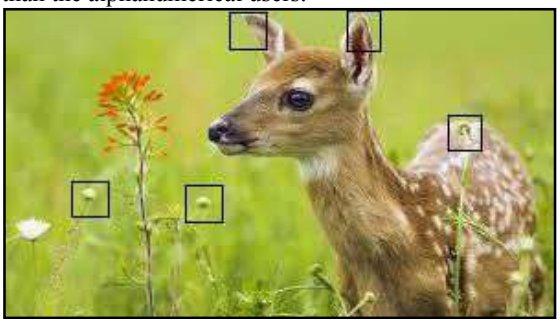
In Cued recall scheme, in which a password is created by making the user click on several locations on an image was at first given by Blonder. Then the pool of neighboring areas of those spots are to be clicked by users during login/authentication. The image can helps users

IJEPAS

International Journal of Engineering, Pure and Applied Sciences,
Vol. 3, No. 1, March- 2018

recollect their password selection memory. Users may select desired items in the image in the exact sequence as registered to be authenticated. Implementation of hidden boundaries for item detection is done to be verified if it was clicked.

In the "PassPoint" system by Wiedenbeck, et al. has extended Blonder's idea of eliminating the predefined boundaries and allowing user to choose random images. In this scheme, a user can click on any place on an image to create a password. A tolerance area around each chosen pixel is calculated. For authentication, the user must click within the tolerance of their chosen pixels and also in the correct sequence. This technique belongs to the discretization method proposed by Birget, et al. Any given picture can be used and because a picture may contain hundreds of thousands of memorable points. Wiedenbeck, et al. conducted a user study in which one group of participants was asked to use traditional alphanumerical password, while the other group was asked to use the image password. The result evaluate that graphical password took less attempts for the user than alphanumerical passwords. However, graphical password users had less difficulty learning the Password, and took less time to input their passwords than the alphanumerical users.



Further study in PassPoint,Wiedenbeck, et al. also conducted a user study to estimate the effect of tolerance square of clicking during the login stage, and the effect of image choice in the system. The result shown that memory accuracy for the graphical password was strongly reduced by using a smaller tolerance for the user clicked points, but the choices of images did not make a significant difference.

5. CUED CLICK POINTS

In Cued Click-Points (CCP) scheme which is proposes alternative to Pass Points. At CCP, users click one point on each of images rather than to five points on one image. It offers oneto-one cueing to user, where each image plays as a cue for the one corresponding click-point, and introduces implicit feedback, where visual cues instantly alert legitimate users if they have made a mistake when entering their latest clickpoint (at which point they can cancel their attempt and having facility of retry from the beginning). As shown in Fig. 2, each click results in showing a next-image, in effect leading users down a path as they click on their sequence of points. A wrong click gives an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image. If users dislike the resulting images, they may create a new password relating different click-points to get different images. Shoulder-surfing is a concern with CCP. It should be noted that obtaining only the sequence of images does not provide enough information to log in directly; considerable additional effort is required to identify where to click on the images to obtain this sequence. A major usability improvement over PassPoints is that genuine users get immediate feedback about an error when trying to log in. When shown an incorrect image, they know that the latest click-point was incorrect and can immediately cancel this attempt and try again from the beginning. Providing explicit feedback in PassPoints before the final click-point could allow PassPoints attackers to increase an online attack to prune potential password subspaces, whereas CCP's visual cues should not help attackers in this way.

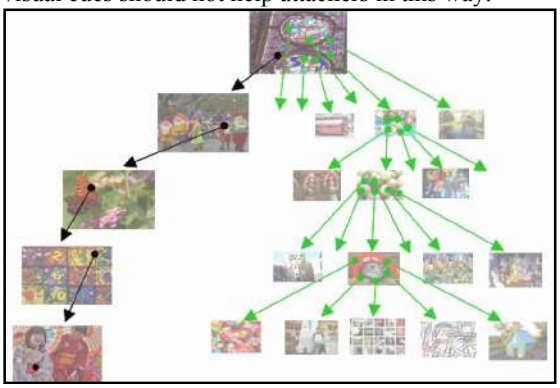


Fig. 2 CCP method

6. PERSUASIVE CUED CLICK POINTS

Pass-Points and cued click points have hotspot problems which reduces the security of graphical password schemes while implementation. To overcome this issues persuasive cued click point's graphical password method was implemented. In PCCP a password was created with five click-points, one click point on each of given five images. During password creation, for a small view port area was provided which is randomly positioned on the image. Users have to select a click-point within the view port. If users are unable or unwilling to select a click point in the current view port, they may press to the Shuffle button to change position the view port randomly. The view port was used as help of users to select more random image passwords that are reduce to hotspots problem. A user who is wants to reach a liked click-point area may still shuffle until the viewport moves to the specific location.

IJEPAS

International Journal of Engineering, Pure and Applied Sciences,
Vol. 3, No. 1, March- 2018

A persuasive cued click point scheme is basically based on Persuasive Technology This technology is used to motivate and provide control to people to behave in a desired manner. Persuasive Technology was first given by Fogg. An authentication system which based on Fogg's Principle of Reduction by making the desired task of choosing a strong password easiest and also provides the Principle of Suggestion by embedding suggestions for a strong password directly within the process of choosing a password.

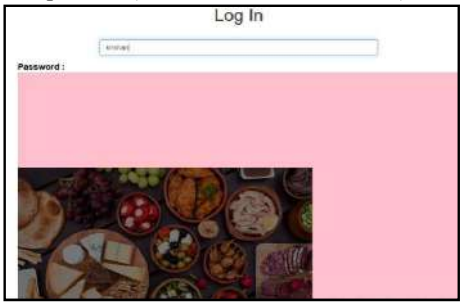
7. PROPOSED SYSTEM

The major challenges to this graphical password model are: spyware and shoulder surfing. Suppose an attacker has somehow installed a web browser addon which is capable of detecting clicked pixels/coordinates on the screen and also the screen size. Then by using an appropriate scaling factor, the person can map those to his screen and the password will be cracked.

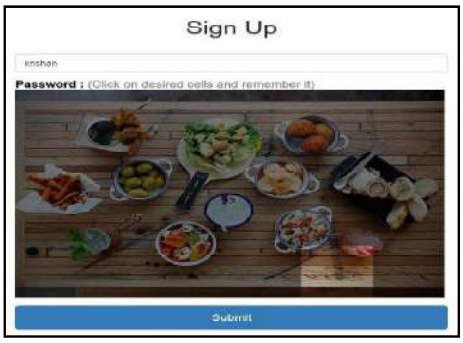
To overcome this, a randomized positioning of the gridded picture is proposed. In this way even if the attacker get the coordinates, mapping to the correct cells is not possible because the image division is not constant. Also, valid users will not be affected because they will always know the position of the registered choices/cells w.r.t picture. In our implementation, we have randomized the 600x400(pixels) image within a 900x600(pixels) background division. If change to adjacent cell is by 100 pixels, then we can move 4 positions horizontally and 3 positions vertically. Thus, a randomization of 12 locations of image positions is possible for each click. Below is a sequence of user interactions for registering and then logging in.

1. Going to the application's home page.

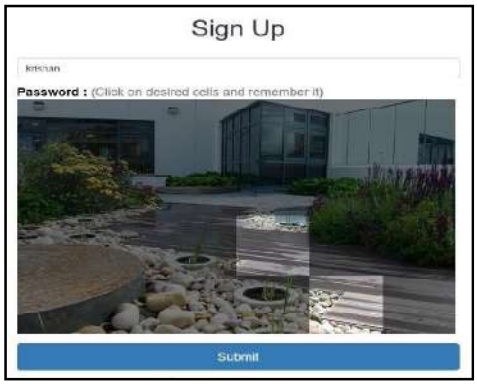
2. Selecting the desired cell from the first. picture. (here username = 'krishan')



3. Selecting desired cell from the second picture.



4. Selecting third cell and logging out.
5. Login as the registered user.



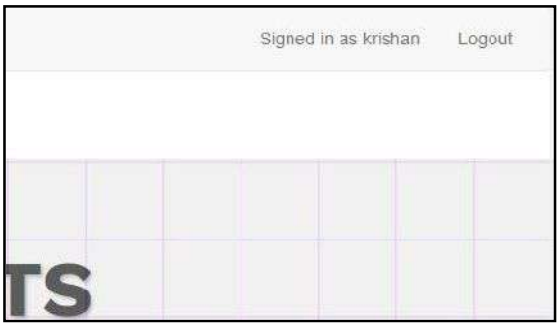
6. Selecting the desired cell from the first picture.

7. Selecting desired cell from the second picture.

International Journal of Engineering, Pure and Applied Sciences,
Vol. 3, No. 1, March- 2018

8. Selecting third cell and back to homepage as signed in user.

Zooming into navbar.



8. RESULT

The model provides significant immunity from detecting click points by spywares or browser addons. The change of position of the gridded image is very random. Additionally, it also provides a little challenge to shoulder-surfing as the image is not static to a side.

9. CONCLUSION

Picture passwords serve as alternative to textual alphanumeric passwords. They fulfill both conflicting requirements of a strong password i.e. they are easy to remember & hard to guess. By the solution of the shoulder surfing problem, it becomes more secure & easier password scheme. Additionally encryption and hashing functions for storing and retrieving pictures and points, one can achieve more security. Picture password is still immature; more research is required in this field. While increasing the number of images and congesting the grids the security will be very high as password space will increase exponentially.

REFERENCES

[1]. G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

[2]. S.Wiedenbeck, J.Waters, J. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies ,2007.

[3]. S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. van Oorschot, "Persuasive cued clickpoints: Design, implementation, and evaluation of a knowledge-based authentication mechanism," School of Computer Science, Carleton University, Tech. Rep. TR-11-03, February 2011.

[4]. S. Chiasson, E. Stobert, A. Forget, R.Biddle, and P. van Oorschot, "Persuasive cued clickpoints: Design, implementation, and evaluation of a knowledge-based authentication mechanism," School of Computer Science, Carleton University, Tech. Rep. TR-11-03, February 2011.

[5]. S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using Cued Click Points," in European Symposium on Research in Computer Security (ESORICS), LNCS4734, September 2007.

[6]. P. C. van Oorschot and J. Thorpe, "Exploitingdictability in click-based graphical passwords," Journal of Computer Secuity, vol. 19, no. 4, pp. 669–70,2011