Floating Captcha Security Technique for authentication

Laiji George

***Abstract*— A CAPTCHA (Completely Automated Public Turing Test to tell computers computer and human apart) challenge using Captcha as graphical password is used as authentication mechanism. In this paper, floating captcha security is integrated to make the system secure. Captcha technique is improved by adding floating capability to Captcha. Apart from floating captcha click animal, captcha zoo and animal grid technologies are also used to enhance security. It eliminates the chances of shoulder surfing attack, image hotspot problem, online guessing attack, human based hacking attack and relay attack. The security can also be improved by generation of Captcha images on different levels of difficulty based on login history and IP address of the machiene. The machiene produces simple captcha challenges for known machienes and complex for unknown one.**

***Index Terms*— authentication, CAPTCHA, Floating Captcha, hotspot, shoulder surfing attack, security.**

I. INTRODUCTION

Security is an inevitable factor to avoid unauthorized access of information. An efficient way to provide security to the computer system is by giving username and password. The choice of password needs a special attention of user. If the user chosen password is weak then it is easily identified through different type of attack such as dictionary attack, guessing attack [1], relay attack and shoulder surfing attack etc. The strength of the password can be improved by using graphical passwords integrating with floating Captcha technology

Graphical password [2] schemes are more reliable and more resilient to dictionary attacks [3] than textual passwords, but more vulnerable to shoulder surfing attacks [4]. Graphical password is an alternative to text password since it is easier for human to remember graphical passsword. By integrating floating feature, the scheme is more resistant to shoulder surfing attack.

The applications of this click based authentication includes security on touch screen devices, e-banking system etc. It also increases spammer's operating cost and thus reduces spam emails. Click based authentications are built on the top of Captcha technology both text Captcha and image recognition Captcha.

Manuscript received January, 2015
***Laiji George** is currently pursuing Masters Degree Program in computerscience and engineering in MP Nachimuthu M Jaganathan Engineering college, erode- Annauniversity India.*

*In this scheme a small threshold is applied for failed login attempts from unknown machiene and large threshold is applied for failed attempts from known machiene where successful login happened within time frame*In this paper a new security primitive is introduced by the combination of floating text, click animal and animal grid. The Captcha technology is incorporated with floating security technique. The hybrid combination of floating Captcha and graphical passwords enhances the level of security. When one Captcha scheme is broken the other with more security can be used to convert to the described scheme. The system has the capability to produce simple captcha challenges for known and complex for unknown machienes.

II. LITERATURE REVIEW

2.1. Graphical Password

The graphical password technoques are mainly classified in to three based on the nature of memorizing passwords. They are recognition, recall and cued recall. In recognition based system the user need to identify the Captcha from image portfolio. In passface system [5] the user has to identify the faces of human being. Another rcognition based scheme which is based on color image gallery is Dejavu [6]. Here the password space is the combination colors.

In recall based scheme the user has to remember the previously defined interaction with th system. Draw A Secret [7]is a recall basecd scheme the user has to draw the pattern on the provided grid space. In Pass Go system user has to click on grid intersection rather than grid cells. Click A Secret is scheme where the user is supposed to click on the grid cells to authenticate the user.

In cued recall system an external cue is provided to help the user to memorize the password. Passpoints [8]is such a scheme where user click on images to generate password and has to reclicks the same sequence on authentication. In Cued Click Points [9] a sequence of images are used and user has to click once in an image. An improvement on CCP is Persuasive Cued Click Points [10], here the user is provided with a viewport to click on the images. The remaing portions otherthan view ports are shades

2.2. Captcha

Captcha relies on gap of capabilities between human and machiene in solving hard AI problems.the Captcha are divided

ISSN: 2278 – 7798

in to text Captcha and image recognition Captcha. Text Captcha relies on character segmentation while image recognition Captcha relies on object segmentation. Text Captcha [10] is normal Captcha challenge to identify characters. An IRC scheme is Assira [11] meant to identify all the cats from the panelof animals displayed on cluttered background. It relies on the identification on one type of image objects. Captcha can protect sensitive user input on an untrusted client [12]. t protect channel of communication between user and webserver from spywares [13].

2.3 *Floating Captcha*

Captcha security technique is improved by adding floating ability to our Captcha scheme. The Captcha characters and objects are made to float on the screen. The users need to recognize their Captcha characters which are floating on the screen. This scheme is more resistant to shoulder surfing attack.

III. CLICK BASED AUTHENTICATION

In click based authentication scheme against spyware a new image is generated for every login attempt of the user which is a Captcha challenge. For normal Captcha challenges user have to identify and enter the given text. In this scheme the user has to click on the Captcha challenges to make his own password. The password generation is a stepwise procedure. It is the combination of both graphical password and floating Captcha. According to the task in memorizing password the authentication scheme is categorized as recognition based scheme which requires recognizing an image and using recognized objects as cues to enter password.

The user has to enter unique userid for his account and is stored in authentication server. The authentication server stores a salt value s and hash value using salt and password for each user id. On authentication request user is provided with Captcha challenge and the user has to enter the click points on the images. The userid along with click points recover the hash value and is compared with the stored hash value.

3.1 RECOGNITION BASED SCHEME

In recognition based scheme an infinite number of visual objects can be accessed as password. Objects in Captcha challenges are arranged at different levels and the user has to recognize those objects and click on the objects in the correct order to authenticate the user with the system. Floating Captcha Text, Captcha Zoo, Click Animal, Animal Grid are the different approaches used in this scheme.

3.1.1. Floating Text Captcha

Floating text Captcha is recognition based authentication scheme consist of characters with out any visually confusing characters. It is the sequence of characters and is entered by click points on the characters. A click text can be produced by any Captcha engine and the location of characters is tracked to produce location of the character in the generated image. The characters are floating in the screen. The authentication server identifies the characters based on their click points. In entering a password the user clicks on the image in the same order as he entered during registration

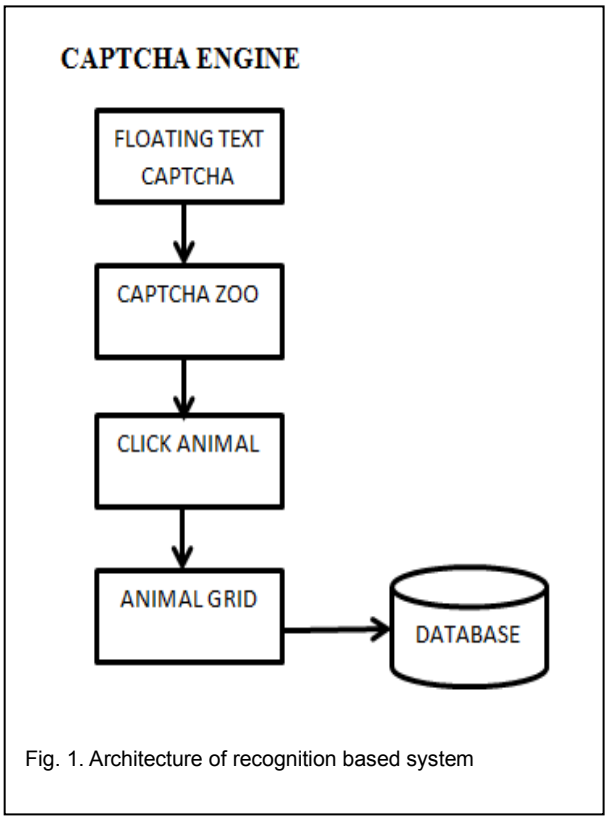

Fig. 1. Architecture of recognition based system

3.1.2 Captcha Zoo

After entering click text password the next stage of Captcha challenge is Captcha zoo [14]. In this level of Captcha challenge the user is provided with animals arranged on a cluttered background. This Captcha scheme consists of 3D models of horse and dog to generate 2D animals with different textures, poses and colors. A user has to identify all the horses or dogs in the cluttered background. This level is a test to identify whether the user is a human or machiene.

3.1.3 Click Animal

The next step in authentication system is click animal. Click animal is built on the Captcha zoo technology. This scheme is based on non character recognition. The images of different animals like cat, dog, horse, camel, turkey arranged on a grassland background. The password set consists of sequence of animals. It is harder for the computer to recognize the animals in the generated image, yet humans can easily identify different instantiations of animals.

3.1.4 Animal Grid

The next step in recognition based authentication is animal grid. Click animal password space is very smaller since the number of animals is limited and thus vulnerable to guessing attack.To resist this type of attack click animal password space

ISSN: 2278 – 7798

can be increased by combining it with a grid based graphical password, with the grid depending on size of animal. Animal grid is a combination of click animal and clicks a secret (CAS) where user click grid cells in her password.

The click animal Captcha challenge appears for clicks on each combination of animals. A grid cell will appear and then the user has to select numbers from those grid cells. If the click animal step is wrong then follow-up grid will be wrong. So it is difficult for the attacker to break the password. A click on th correctly labeld grid-cell of the wrong grid would likely produce a wrong grid-cell at the authentication server side when the correct grid is used.

For the user to enter password, a click animal image is displayed first and after selecting the combination of animals an image of n x n grid appears. Grid cell size is equal to the bounding rectangle of animal. The each grid cell is labeled with numeric for the user to identify the cells. The grid cell pattern depends on the first animalthat the user clicked. Grid cell differ for different animals. The co-ordinates of the grids are located and checked with authentication server. The server recovers the first animal from the received sequence, regenerates the grid image from the animal's bounding rectangle and recovers the password user clicked.

3.2 captcha in authentication

In this scheme we use both floating Captcha and password in a user authentication protocol which is also called Captcha based Password Authentication Protocol, to counter online dictionary attack. This protocol involves solving Captcha challenge after inputting a valid pair of userid and password. The co-ordinates of the clicked points are hashed with the salt value and stored in the database. On each login attempt the hash value is regenerated from the click points and compares with the stored hash value corresponding to each userid.

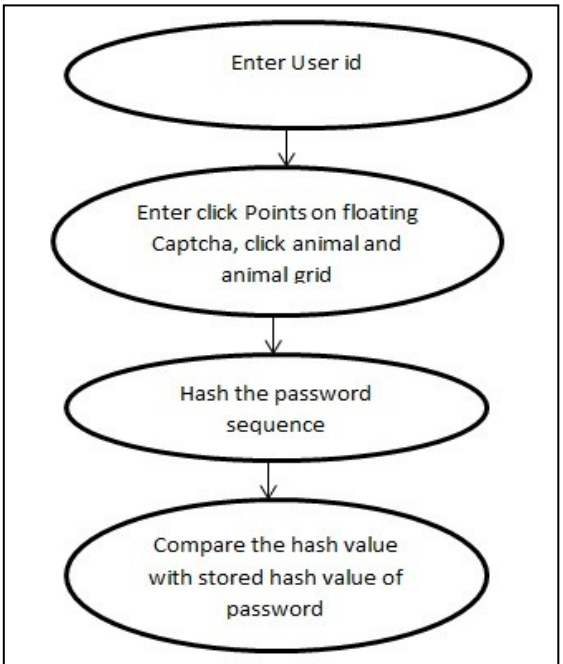

Fig. 2. Flow chart of click based authentication system

The Captcha challenges generated at different levels of difficulty based on the user. If the user tries to login from known machiene then a regular Captcha challenge is generated. otherwise the user loggedin from an unknown machiene and then user has to solve difficult Captcha challenge based on the threshold value of wrong attempts. The only difference is hard image is generated in latter case and easier in former case.

IV. DISCUSSION

4.1 captcha security

The click text password consists of 30 or more characters. The Captcha challenge that we normally used consist of only 6 to 8 characters. The spyware attack is removed by adding floating technology. The complexity to break the click text is very large compared to the traditional Captcha challenge. Thus it is harder to break than its underlying Captcha scheme. Click animal relies on both object segmntation and multiple label classification. If one Captcha scheme is broken other Captcha schemes can be used.

4.2 Guessing attack

The guessing attack is done by trial and error method. A password guess is tested in an unsuccessful trial is considered as wrong from subsequent trials. The recognition based scheme increase password space to make password harder to guess. Automatic online guessing attacks are avoided by using salt value while hashing the password. In human guessing attacks, humans enter the password in trial and error process. The text password we chose is between 6-8 characters and he has strong dislike towards alphanumeric characters. The complexity to break click text Captcha is α^{30} P(N)/(α^{10} P(N))= α^{20} times the complexity to break text captcha In this case click text and animal provide better password space. Each trial in human guessing is computationaly independent of other trials. No matter how many trials executed the number of trials remains the same

4.3 Relay attack

In this type of attack requires human surfers to solve Captcha challenges in order to continue surfing the website. The task to solve and the image used in the Captcha as graphical password scheme are very different from normal Captcha challenge. Therefore it is more harder to get a large number of unwitting people to mount human guess attack on click based authentication scheme. The human input is obtained by a sequence of Captcha task on the Captcha challenge images is useless for testing a password guess.

4.4 Shoulder surfing attack

However shoulder surfing attack is threat to this scheme when passwords are entering in public place. In this scheme integrating floating capability to Captcha make it resistant to shoulder surfing attack. The click based authentication scheme

ISSN: 2278 – 7798

on combination with dual viewing technology can successfully eliminate the attack through shoulder surfing. The higher the correlation of user clicked points between various login attempt, the dual viewing technology protection strategy needed is less. The floating technology improves the security of Captcha technology.

V. CONCLUSION

Captcha is both a captcha and graphical password scheme. A new family of password consists of Captcha challenges with floating character images and non character images. For every login attempt a new Captcha image is appeared which is floating in the screen. For every login attempt a new captcha challenge is appares and the co-ordinates are hashed to counter hacking attacks. It increases spammers operating cost and thus reduces spam emails.The security is enforced at different stages of captcha such as floating captcha, click animal, captcha zoo and animal grid. The usability can be further improved by using images with different levels of difficulty based on login history and machiene. Captcha challenge does not rely on any specific Captcha scheme. When one scheme is broken a more secure scheme can be used. It is more resistant to human based attacks.

Because of reasonable security and usability of practical applications, integrating floating captcha to graphical passwords has good potential for future works.

ACKNOWLEDGMENT

I would like to thank Mr. K.N Sivakumar, HOD, Department of Computer Science and Engineering my guide Ms. P. Shenmbagavalli, Assistant Professor, Department of Computer Science and Engineering and Mr. Anoop T.K, Bodhi Info Solution for their wonderful support throughout this project.

REFERENCES

[1] M. Alsaleh, M. Maman and P.C Van Oorschot, "Revisiting defenses against largscle online password guessing attacks,"*IEEE Trans. Dependable Secure Computing*, vol 9. No.1 pp.128-141, 1989.

[2] S. Chiasson, P. C. van Oorschot, and R. Biddle," *Learning from the first twelve years," ACM Comput. Surveys*, Vol.44 no.4 2012

[3] P. C. van Oorschot and S. Stubblebine, "On countering online dictionary attacks with login histories and humans-in-the-loop," *ACM Trans. Inf. Syst. Security*, vol. 9, no. 3, pp. 235–258, 2006.

[4] S. Kim, X. Cao, H. Zhang, and D. Tan, "Enabling concurrent dual views on common LCD screens," in *Proc. ACM Annu. Conf. Human Factors Comput. Syst.*, 2012, pp. 2175–2184.

[5] (2012, Feb.). *The Science Behind Passfaces* [Online]. Available: http://www.realuser.com/published/ScienceBehindPassfaces.pdf

[6] R. Dhamija and A. Perrig, "Déjà Vu: A user study using images for authentication," in *Proc. 9th USENIX Security*, 2000, pp. 1–4.

[7] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in *Proc. 8th USENIX Security Symp.*, 1999, pp. 1–15.

[8] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in *Proc. ESORICS*, 2007,pp. 359–374.

[9] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better passwords: Persuasive cued click-points," in *Proc. Brit. HCI Group Annu. Conf. People Comput., Culture, Creativity, Interaction*, vol. 1. 2008, pp. 121–130.

[10] K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski, "Building segmentation based human-friendly human interaction proofs," in *Proc. 2nd Int. Workshop Human Interaction Proofs*, 2005, pp. 1–10.

[11] J. Elson, J. R. Douceur, J. Howell, and J. Saul, "Asirra: A CAPTCHA that exploits interest-aligned manual image categorization," in *Proc. ACM CCS*, 2007, pp. 366–374.

[12] M. Szydlowski, C. Kruegel, and E. Kirda, "Secure input for web applications," in *Proc. ACSAC*, 2007, pp. 375–384.

[13] H. Gao, X. Liu, S.Wang, and R. Dai, "A new graphical password scheme against spyware by using CAPTCHA," in *Proc. Symp. Usable Privacy Security*, 2009, pp. 760–767.

[14] 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

Laiji George *is currently pursuing Masters Degree Program in computerscience and engineering in MP Nachimuthu M Jaganathan Engineering college, erode- Annauniversity India, Member of Computer Society of India*

ISSN: 2278 – 7798