www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 4 April 2015, Page No. 11487-11490

Captcha as Graphical Password

Sujata D. Salunkhe[1], Prof.Dhanshree Patil[2]

[1]PG student,
Nutan Maharashtra Institute of Engineering and Technology,
Talgaon Dabhade,Pune.
sujatasalunkhe5@gmail.com

[2]Department of Computer Engineering
Nutan Maharashtra Institute of Engineering and Technology,
Talgaon Dabhade,Pune.
patildhanshri@gmail.com

Abstract:-Security is the primitive issue in all the areas related to computers. Proper authentication is required to make the network secure. The traditional way of password using characters is vulnerable and easy to hack. So that method is integrated with new paradigms, such as Graphical Password, Captcha. Still the technology is evolving, a new security primitive based on hard AI problem, called Captcha as Graphical Password is evolving. CaRP is the combination of both Captcha and Graphical Password which make it hard to intruders to hack the password.

Keywords: Captcha, CaRP, Graphical Password, Authentication

1. Introduction:-

For security hard AI (Artificial Intelligence) problems are used. Using the paradigm, the most notable primitive is Captcha. Captcha is “Completely Automated Public Turing test to tell Computers and Humans Apart” which distinguishes human users from computers by presenting a challenge.

The challenge is beyond the capability of computers but easy to humans. A new security primitive based on hard AI problems, graphical password systems integrating Captcha technology, which is called as CaRP(Captcha as gRphical Password) is evolved [1]. CaRP is click based graphical password system, where a sequence of click on images is used to define a password. CaRP can be used in:

1. CaRP can be applied on touch screen devices for typing password for secure banking application.
2. CaRP increases spammer’s operating cost and thus helps reduce spam emails. An email service provider who deploys CaRP, a spam bot cannot log into an account even if it knows the password. Human involvement is necessary to access an account.

2. Background

2.1 Graphical password

A Graphical Password system [2] is of three types as:

1. Recognition Based scheme
2. Recall Based scheme
3. Cued Recall Based scheme

2.1.1 Recognition Based scheme

A recognition based scheme identifies among group of visual objects belonging to a password portfolio. Passfaces is the most widely used scheme. Where a user selects a portfolio of faces from a database in creating a password. While authentication, a panel of candidate faces is presented for the user to select the face belonging to his portfolio. This process is repeated several rounds, with a different panel for each round. Correct selection in each round tends to successful login. In Cognitive Authentication user generate a path through a panel of images –starting from the top left image ,moving down if the image is the portfolio, or right otherwise.

2.1.2 Recall Based scheme

In recall based scheme user has to regenerate the same interaction result without cuing. Draw-A-Secret is the well known scheme. A 2D grid is provided to draw a password. The system encodes the sequence of grid cells along the drawing path. Pass-Go [5] is another integrated version of DAS where grid intersections are encoded instead of grid cells.

2.1.3 Cued Recall Based scheme

Pass Points is a click based cued recall scheme where a user requires clicking a sequence of points anywhere on an image to create a password. At the time of authentication user require to click at the same points as the password. Cued

Click Points (CCP) [9] is another scheme where one image per click is used. Persuasive Cued Click Points (PCCP) extends CCP where user has to select a point inside a randomly positioned viewport.

2.2 Captcha

Captcha is the abbreviation for "Completely Automated Public Turing Test to tell Computers and Human Apart". Captcha finds the difference between humans and bots in solving the hard AI problems. It is a test to check user is Human and not a computer device .Captcha is of two types: Text Captcha which is recognition of non-character objects and Image Recognition Captcha relies on recognition of images [3] .

2.2.1 Text Captcha

PayPal and Microsoft Captcha are both relied on background noise and random character strings to resist automated attacks. . The Captchas used by Google,Yahoo! all share similar properties: such as a lack of background noise, distortion of characters or word images and extreme crowding of adjacent character. The human readability of random Captcha images is captured by site in the form of pixel, marginal probabilities and site by site covariance [3]. EZ-Gimpy uses word images which employ character distortion and clutter. Pessimal Print uses a low quality images by degrading parameters to thicken, crowd, fragment and add noise to character images. These Captchas are shown in Fig.1

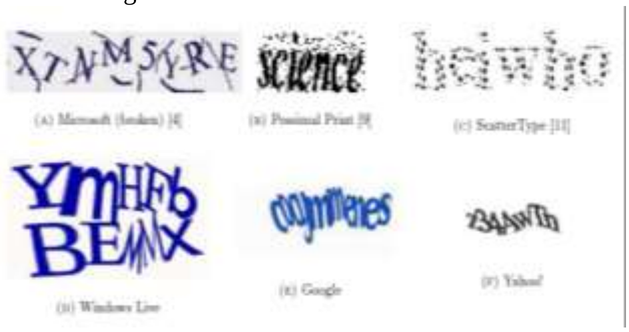

Fig. 1 Captcha examples

2.2.2 Image Recognition Captcha

These Captcha consist of combination of images [6]. User has to recognize the images given to him to solve the given puzzle. As shown in Fig. 2 user has to select the cat images as the password characters.

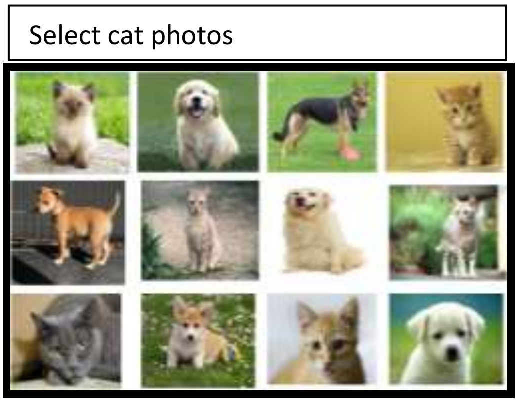

Fig 2. Image Based Captcha

3. Captcha as Graphical Password

CaRP is the integration of both Captha and Graphical Password [1]. For every login attempt a new image is generated. CaRP generate a image using an alphabet of visual objects(e.g. similar animals) . The visual objects in the alphabet are different in CaRP image and Captcha image though both are presented as a challenge to the user.

3.1 Authentication process in CaRP Schemes

A CaRP password is a sequence of visual objects IDs or clickable points of visual objects that user selects. The authentication server AS stores a salt s and hash value H(ρ,s) for each user where ρ is the password. When a user attempts to login, AS generate a CaRP image,records the locations of the objects in the image, and sends the image to the user to click the password. The clickes coordinates are recorded and passed to AS along with user ID. AS matches the received co-ordinates onto a CaRP image which user clicked with the clickable points of visual objects of ρ. Then AS retrives salt s of the account, calculates the hash value of ρ with the salt, and compares the result with the hash value stored for the account. If the two hash value matches, it means that the authentication is successful. The above explained CaRP authentication process can be shown diagrammatically as in Fig. 3.

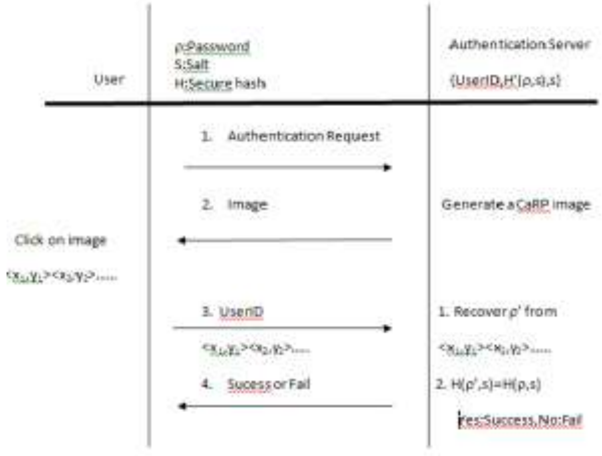

Fig.3 Flowchart of basic CaRP authentication

3.2 Recognition based CaRP

Following are the types of recognition based CaRP, where a password is a sequence of visual objects.

3.2.1 ClickText

ClickText image is similar to a Captcah image and is generated by Captcha engine. A ClickText password is a sequence of characters in the alphabet, e.g. "CD23MT@7". The CaRP alphabet characters should appear in the image. In ClickText images, characters are randomly arranged on 2D space as shown in Fig. 4. The figure contains alphabet of 33 characters. While entering the password user clicks the character on the image in the same order, for example, "C","D","2","3","M","T", "@","7" for the password ρ="CD23MT@7".

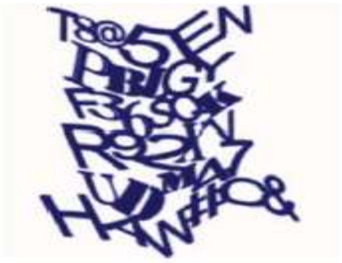

Fig. 4 ClickText image with 33 character

3.2.2 ClickAnimal

ClickAnimal is a recognition based scheme with an aplphabet of somilar animals. The password is a sequence of animal names such as ρ=”Horse,Dog,Cat,…”. 3D models are used to generate 2D animals by applying different views, textures,,colors, lighetning effects and optionally distortions. The resulting 2D animals are arranged on background such as grassland. Some animals may be overlapped by the other animals but they can be easily identifyed by humans. Fig 5 shows a ClickAnimal image with 10 animals.

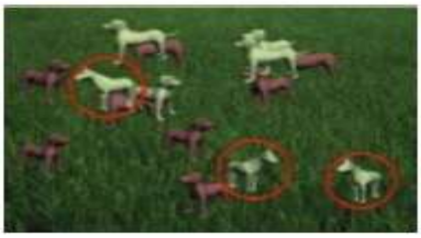

Fig. 5 ClickAnimal image with Horse circled red

3.2.3 AnimalGrid

AnimalGrid is integration of ClickAnimal and CAS. The process of entering password is follows… A ClickAnimal image is displayed first. When user selects an animal, an image of n × n grid is displayed with the grid cell size equalling the bounding rectangle of the selected animal. Fig. 6 shows a 6 × 6 grid. A user can select zero or multiple grid cells matching her password. So, the password is a series of animals interleaving with grid cells. E.g. “Dog, Grid_2, Grid _1,Cat,Horse,Grid_3” where Grid_1 means the grid cells indexed as 1.Grid cells after an animal means that grid is determined by bounding rectangle of the animal.

When a ClickAnimal image is displayed , the user selects the animal matching the first animal from the password by clicking on the animal. The clicked point’s coordinates are recorded. The bounding rectangle is calculated and displayed. E.g. white rectangle in fig 6. The user corrects the inaccurate edges if any by dragging it. This process is repeated until user satisfaction. After this an image of n × n grid for the bounding rectangle is displayed. Now the user selects a sequence of zero or multiple grid cells that match with grid cells following the first animal in the password,and the go back to ClickAnimal image. The above specified password will result in the sequence as “AP_150,50,GP_30,40,GP_53,130,AP_120,89……” where “AP_x,y” denotes the points of ClickAnimal Image, and “GP_x,y” denotes the points on a grid image. These coordinates are sent to authentication server.

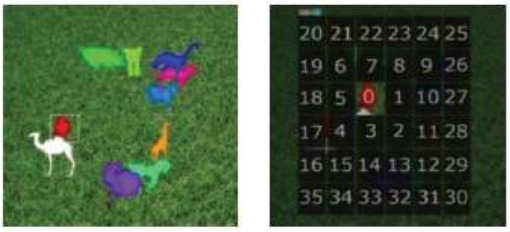

Fig.6 ClickAnimal image with 6 ×6 grid

3.3 Recgnition –Recall CaRP

In recognition-recall CaRP, a password is a sequence of some invariant points of objects. An *invariant point* of an object (e.g. letter “A”) is a point that has a fixed relative position in different incarnations (e.g., fonts) of the object, and thus can be uniquely identified by humans no matter how the object appears in CaRP images.

3.3.1 TextPoints

Fig. 7 shows some invariant points of letter “A”, which offer a strong cue to memorize and locate its invariant points. A set of clickable points for TextPoints is formed by selecting a set of internal invariant points of character. An internal point of an object is the point whosw distance to the closest boundary of the object exceeds a threshold.

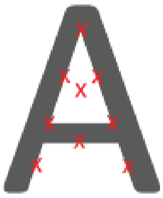

Fig.7 Some varient points with red crosses

The user selects the points among the clickable points marked on corresponding characters in a CaRP image to form a password. While authenticating the user, user first recognize the chosen characters, and clicks the password points. The authentication server matches the user clicked points and closest clickable point. If there is far difference, login fails. Or else hash value of clicked points is calculated to compare with stored value.

3.3.2 TextPoints4CR

The modified version of TextPoint is TextPoint for Challenge Response or TextPoints4CR.

TextPoints4CR stores a password for each account instead of a hash value as in TextPoint. Each character appears only once. An image is partitioned into fixed grid. While entering a password, a user clicked point is replaced by the grid cell it lies in. If click errors are within threshold the user clicked point are same as original password point. Therefore sequence of grid cells generated from user clicked points is identical to the one that authentication server generates from stored password. In this scheme authentication server stores the password instead of hash values. Therefore the password should be protected from insider attacks. So the passwords are encrypted with a master key which is known only to the authentication server. A password is decrypted only when the associated account attempts to log in.

Conclusion:-

CaRP is new technique to provide security to the password using hard AI problems. As it is combination of both Captcha and Graphical password it makes it very hard to guess the password to the intruders or bots. Effective use of both the techniques makes it useful to use it for smartphones and computers accessing the secure applications such banking, mailing ,etc.

References:-

[1] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, "Captcha as Graphical Passwords—A New SecurityPrimitive Based on Hard AI Problems" , IEEE Transactions On Information Forensics And Security, Vol. 9, No. 6, June 2014

[2] Robert Biddle, Sonia Chiasson, P.C. van Oorschot, "Graphical Passwords:Learning from the First Twelve Years" , ACM Comput. Surveys, vol. 44, no. 4, 2012

[3] Michael A. Kouritzin*, Fraser Newton, And Biao Wu, " On Random Field Captcha Generation"

[4] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA:Using hard AI problems for security," in Proc. Eurocrypt, 2003, pp. 294–311.

[5] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292,2008

[6] P. C. van Oorschot and J. Thorpe, "On predictive models and user drawn graphical passwords," ACM Trans. Inf. Syst. Security, vol. 10,no. 4, pp. 1–33, 2008.

[7] P. C. van Oorschot and J. Thorpe, "Exploiting predictability in clickbased graphical passwords," J. Comput. Security, vol. 19, no. 4,pp. 669–702, 2011

[8] 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

[9] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA:Using hard AI problems for security," in Proc. Eurocrypt, 2003,pp. 294–311.

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

[11] D. Davis, F. Monrose, and M. Reiter, "On user choice in graphical password schemes," in Proc. USENIX Security, 2004, pp. 1–11

[12] B. B. Zhu et al., "Attacks and design of image recognition CAPTCHAs,"in Proc. ACM CCS, 2010, pp. 187–200.

[13] 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.

[14] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot spots in graphical passwords," in Proc. USENIX Security, 2007,pp. 103–118.