Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Captcha as a Graphical Password Using Hard AI Problems

Shruti Alai[1] , Sonali Pagar[2] , Yogita Chaudhari[3] , Medha Joshi[4]
[1,2,3,4]*B.E. Student, Department of Computer Engineering,*
Pune Vidyarthi Griha's College of Engineering Nashik, Maharashtra, India

Abstract: ***The new security premitive based on hard Artificial inteligence problems, say as graphical password system built on top of Captcha Technology referred to as "Captcha As a gRaphical Password (CaRP)". CaRP resolves a number of security problems altogether, viz., dictionary attacks, shoulder surfing attacks, online guessing attacks, relay attacks. CaRP also addresses the well-known image as passpoints. Though CaRP does not solve all these security related problems, but it offers reasonable security with some practical applications for improving online security. CaRP is click point based graphical password, in which sequence of clickable points are generated to form a password, and a new CaRP image is generated for every login attempt even for the same user.***
Keywords: Graphical Password, Captcha, CaRP, Shoulder surfing, online guessing attacks, passpoints.

I. INTRODUCTION

A. Graphical Passwords

Till now a large number of graphical password schemes have been introduced. They are classified into three broad categories according to the task involved in memorizing and inputing passwords: recognition, recall, and cued recall. It is required for a recognition-based scheme that identify among attractive visual objects belonging to a password range. A typical scheme is Passfaces wherein a user selects a group of faces from a database for creating a password. While doing authentication, a panel of candidate faces is presented for the user to select the face belonging to her group. This process is repeated several times, each time with a different panel. A successful login requires proper selection each time. The set of images in a panel remains the same between logins, but their positions are formed by the permutation. The process is similar to Pass faces but the images in the portfolio are ordered, and a user must identify her group images in the proper order. Cognitive Authentication requires a user to generate a way through a panel of images as follows: start from the top to left image, moving down if the image is in her group ,or right otherwise. The user identifies among fake the row or column label that the way ends.

This process is repeated, each time with a different panel. A successful login requires that the simple probability that correct answers were not entered by chance exceeds a threshold within a given number of rounds. In the recall-based scheme user need to regenerate the same result with no cueing. The first recall-based scheme was Draw-A-Secret (DAS). A user draws the password on a 2D grid. The system encodes a sequence of grid cells along the drawing path as a user drawn as a password. Pass-Go improves usability of DAS's by encoding the grid intersection points instead of grid cells. BDAS adds background images to DAS to help users to create more complex passwords. In the cued-recall scheme to remember the password an external cue is provided. PassPoints is another click-based cued-recall scheme where in user clicks the sequence of clickable points where an image creates a password, and again clicks the same sequence of points while authentication. Cued Click Points (CCP) is same as to PassPoints but uses one image for each click, where deterministic function selects next image. credible Cued Click Points (PCCP) enlarge CCP where user have to select a point inside a randomly placed viewport at the time of creating a password. Thus it results in more randomly scattered click-points in the password.

Captcha is based on the gap of capabilities between humans and bots to solve certain hard AI problems. There are two types of visual Captcha : text Captcha and Image-Recognition Captcha (IRC). The previous one based on character recognition while the latter relies on recognition of non-character objects. Security of text Captcha has has been widely studied . The following principle has been established: text Captcha should depends on the difficulty of character segmentation, which is computationally expensive and combinatorially hard . Machine recognition of non-character objects is extreme less capable than character recognition. IRCs depends on the difficulty of object identification is possibly combined with the difficulty of object segmentation. Asirra relies on binary object classification: a user is asked to identify all the dogs from a panel of 12 images of cats and dogs. Security of IRCs has also studied. Asirra was found to be susceptible to machine-learning attacks . IRCs based on binary object classification otherwise

identification of one concrete type of objects are likely insecure . Multi-label classification problems are considered much difficult than binary classification problems. Captcha can be circumvented through relay attacks whereby Captcha challenges are convey to human solvers, whose answers are sent to the targeted application.

II. CAPTCHA IN AUTHENTICATION

It was introduced in to use the both Captcha and password in a user authentication protocol,that is Captcha-based Password Authentication (CbPA) protocol, to counter online dictionary attacks.when a valid browser cookie is received The CbPA-protocol in requires solving the Captcha challenges after inputting a valid pair of user ID and password . For an invalid pair of user ID and password, the user has possible probability to solve a Captcha challenge before being without access. An improved CbPA-protocol is proposed in by storing cookies only on user-trusted machines and apply the Captcha challenges only when the number of failed login attempts for the account has exceed a threshold value. It is further improved in by applying a small threshold value for failed login attempts from unknown machines but a large threshold value for failed attempts from known machines with a previous successful login within a given time frame. Captcha was also used with the recognition-based graphical passwords to address spyware where in a text Captcha is displayed each image; a user locates his own pass-images from lure images, and enters the characters at specific locations of the Captcha below each pass-image as user password during authentication. These specific locations were selected for each pass-image during the password creation as a part of the password. In the above schemes,Captcha is an independententity then used together with a text or graphical password. On the witherward, a CaRP is both a Captcha and a graphical password scheme, which are basically combined into the single entity.

In this system, a new image is generated for each login attempt, even for the same user. CaRP uses an alphabet of visual objects for generating CaRP image, which is also a Captcha challenge. Difference between CaRP images and Captcha images are that all the visual objects in the alphabet should appear in a CaRP image for a user to give input any password & the same is not necessary in Captcha image. Many Captcha schemes can be converted to CaRP systems, as described in the next part. CaRP schemes are clicked-based graphical passwords. According to memory tasks to reminder and inputing a password, CaRP schemes are classified into two categories: recognition and recognition-recall, which requires recognizing an image and using the recognized objects as a sequence to enter a password. Recognition-recall associates the tasks of both recognition and cued-recall, and retain both of these two recognition-based advantage of being easy for human memory and the cued-recall advantage of a huge password space. excellent CaRP schemes of each type will be presented later.

III. CONVERTING CAPTCHA TO CARP

Any visual Captcha scheme relying on recognizing two or more predefined types of objects that can be converted into a CaRP. All text Captcha schemes and most of the IRCs fulfills this requirement. Those IRCs that are based on recognizing a single predefined type of objects can be converted to CaRPs by adding more types of objects. Conversion of a speci?c Captcha scheme to a CaRP system requires a case by case study, in order to ensure both the security and the usability. Several CaRP schemes built on top of text and image-recognition Captcha schemes is described further. Some IRCs rely on identifying objects whose types are not predefined.

The ClickText is recognition-based CaRP scheme built on the top of text Captcha. Its alphabets comprises characters without any visually-confusing characters and text. For example, Letter “l” and digit “1” may cause confusion in CaRP images, and thus one character should be removed from the alphabet. A ClickText password is a sequence of characters in the alphabet, e.g., ? =“AB#2CD86”, which is similar to a text password. A ClickText image is generated by the underlying Captcha engine as if the Captcha image were generated excepting that all the alphabet characters should appear in the image. During generation, each and every character’s location is tracked to produce ground truth for the location of the letters in the generated image. The authentication server depend on the ground truth to identify the characters corresponding to user-clicked points.

The Click Animal Captcha Zoo is a Captcha scheme which is used 3D models of horse and dog to generate 2D animals with different backgrounds such as textures, colors, lightings and poses, and arranges them on a cluttered . ClickAnimal is a recognition-based CaRP scheme built on top of the Captcha Zoo with in an alphabets of similar animals such as dog, horse, pig,cow etc. Its password is a sequence of animal names such as “ Cat, Horse, Dog,cow….” For each animal, one or more 3 Dimentional models are built. The Captcha generation process is applied for generating ClickAnimal images: 3D models are used to generate 2 Dimentional animals by applying different views, textures, colors, lightning effects, and optionally distortions on background. The resulting 2D animals are then arranged on a tangled background such as texture. Some animals may be closed by other animals in

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

the image, but their centre parts are not obstructed inorder for humans to identify each of them. a Click Animal image with an alphabet of 20 animals. Combined with the additional anti-recognition process applied in the mapping step, these make it hard for the systems to recognized animals in the generated image, humans can easily identify different instantiations of animals.

A. System Design

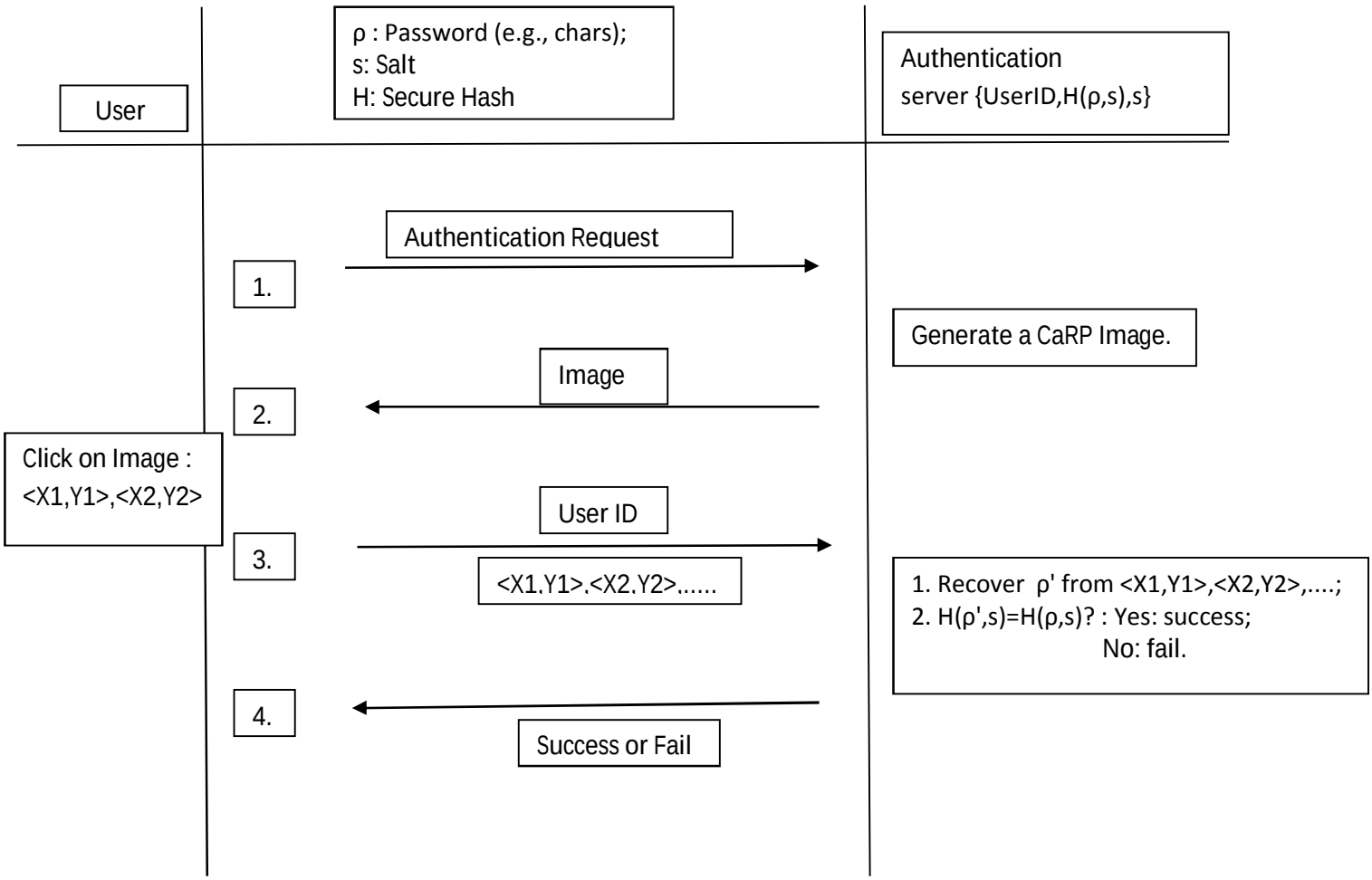

Fig 1. Flowchart of basic CaRP authentication.

IV. ANIMAL GRID

The number of similar animals is lesser than the number of available characters. Click Animal has smaller alphabet, thus smaller password space, than ClickText. In order to avoid human guessing attacks CaRP should have a enough-large effective password space. The password size of AnimalGrid can be increased by combining it with a grid-based graphical password, with the grid depending on size of the animal which is selected. DAS is a candidate which requires drawing on grid. To be consistent with ClickAnimal, it changes from drawing to clicking. Click-A-Secret (CAS) where a user clicks the grid cells in their password. AnimalGrid is formed by combining ClickAnimal and CAS. The number of grid-cells in a grid should be larger than the alphabet size. Unlike DAS, grids in our CAS are object-dependent. It has advantage that a correct animal should be clicked in order for clicked grid-cells which are on the follow-up grid to be correct. If an incorrect animal is clicked, the follow-up grid is wrong. Click on the correctly labeled grid-cell of the wrong grid will be produced a wrong grid-cell at the authentication server side if the correct grid is used. A ClickAnimal image is displayed first to input a password. As soon as an animal is selected, an image of n×n grid is displayed, with the equaling grid-cell size of bounding rectangle of the selected animal. Each grid-cell is labeled to help users

identify.

V. AUTHENTICATION

when user enters a password, a user-clicked point is replaced by the grid-cell it lies in. If click errors are within t,each user-clicked point falls into the identical grid-cell as the original password point. Therefore the sequence of grid-cells generated from user-clicked points is same to the one that the authentication server generates from the saved password of the account. This sequence is used as if the shared secret between the two parties in a challenge-response authentication protocol.

VI. CONCLUSION

Graphical password are an alternative to textual alphanumeric password .It satisfies both conflicting requirements that means easy to remember and hard to guess by the solution of the shoulder surfing problem, it becomes more secure and easier password scheme. by implementing other special geometric configuration like triangle and movable frame, one can achieved more security.

REFERENCES

[1] M. Bertalmio, G. Sapiro, V. Caselles, and C. Ballester, “Image inpainting”, in Proc. SIGGRAPH, pp. 417–424, 2000.
[2] A. Criminisi, P. Perez, and K. Toyama, “Region filling and object removal by exemplar-based image inpainting.”, IEEE Transactions on Image Processing, vol. 13, no.9, pp. 1200–1212, 2004.
[3] Marcelo Bertalmio, Luminita Vese, Guillermo Sapiro, Stanley Osher, “Simultaneous Structure and Texture Image Inpainting”, IEEE Transactions On Image Processing, vol. 12, No. 8, 2003.
[4] Yassin M. Y. Hasan and Lina J. Karam, “Morphological Text Extraction from Images”, IEEE Transactions On Image Processing, vol. 9, No. 11, 2000
[5] Eftychios A. Pnevmatikakis, Petros Maragos “An Inpainting System For Automatic Image Structure-Texture Restoration With Text Removal”, IEEE trans. 978-1-4244-1764, 2008
[6] S.Bhuvaneswari, T.S.Subashini, “Automatic Detection and Inpainting of Text Images”, International Journal of Computer Applications (0975 – 8887) Volume 61– No.7, 2013
[7] Aria Pezeshk and Richard L. Tutwiler, “Automatic Feature Extraction and Text Recognition from Scanned Topographic Maps”, IEEE Transactions on geosciences and remote sensing, VOL. 49, NO. 12, 2011
[8] Xiaoqing Liu and Jagath Samarabandu, “Multiscale Edge-Based Text Extraction From Complex Images”, IEEE Trans., 1424403677, 2006
[9] Nobuo Ezaki, Marius Bulacu Lambert , Schomaker , “Text Detection from Natural Scene Images: Towards a System for Visually Impaired Persons” , Proc. of 17th Int. Conf. on Pattern Recognition (ICPR), IEEE Computer Society, pp. 683-686, vol. II, 2004
[10] Mr. Rajesh H. Davda1, Mr. Noor Mohammed, “ Text Detection, Removal and Region Filling Using Image Inpainting”, International Journal of Futuristic Science Engineering and Technology, vol. 1 Issue 2, ISSN 2320 – 4486, 2013
[11] Uday Modha, Preeti Dave, “ Image Inpainting-Automatic Detection and Removal of Text From Images”, International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622 Vol. 2, Issue 2, 2012
[12] Muthukumar S, Dr.Krishnan .N, Pasupathi.P, Deepa. S, “Analysis of Image Inpainting Techniques with Exemplar, Poisson, Successive Elimination and 8 Pixel Neighborhood Methods”, International Journal of Computer Applications (0975 – 8887), Volume 9, No.11, 2010