International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

Captcha As Graphical Password

Sharwari Parade[1], Rujuta Pachpande[2], Supriya Deshmukh[3], Stuti Ahuja[4]

[1]BE Student, Dept. of Information Technology, Mumbai, India
[2]BE Student, Dept. of Information Technology, Mumbai, India
[3]BE Student, Dept. of Information Technology, Mumbai, India
[4]BE Guide, Dept. of Information Technology, Mumbai, India

---***---

Abstract - *Security is an important issue to tackle. Different user authentication techniques are available for this purpose. Following is the security primitive based on hard AI problems. This technique is based on Captcha technology named Captcha as graphical passwords (CaRP). CaRP is combination of both a Captcha and a graphical password. System which is used currently is based on text or alphanumeric password which is used very commonly and easy to guess. Various attacking techniques are available to hack the password like dictionary attack shoulder surfing attack and brute force attack. CaRP provides a novel approach that addresses image hotspot problem which is encountered in graphical password system like pass points that often leads to choice of weak password. CaRP is not a final solution but offers pretty good security and fits well with many practical applications for better online security.*

***Key Words*: Graphical password, CaRP,Captcha, dictionary attack, password guessing attack, security primitive. CaRP, click based authentication, recognition based validation, Hash visualization, usable security.**

1.INTRODUCTION

Security is most important in our daily life. CAPTCHA stands for Completely Automated Public Turing test to tell Computer and Humans part.

It is essential for accessing confidential data and security parameters were done based on the cryptography and mathematical calculation. tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also be easily guessed or broken. According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords. On the other hand, passwords that are hard to guess or break are often hard to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts. To address the problems with traditional username- password authentication, alternative authentication methods, such as biometrics have been used. However, we will focus on another alternative, using pictures as passwords.

Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots. However, this new paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications. Is it possible to create any new security primitive based on hard AI problems? This is a challenging and interesting open problem. In this paper, we introduce a new security primitive based on hard AI problems, namely, a novel family of graphical pass-word systems integrating Captcha technology, which we call CaRP (Captcha as gRaphical Passwords). CaRP is click-based graphical passwords, where a sequence of clicks on an image is used to derive a password. Unlike other click-based graphical passwords, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every login attempt. The notion of CaRP is simple but generic. CaRP can have multiple instantiations. In theory, any Captcha scheme relying on multiple-object classification can be converted to a CaRP scheme.

2. BACKGROUND

2.1 Graphical Password

Graphical password is the method used as alternative of traditional passwords. In graphical passwords, pictures are used which makes easy to memorize the password. Many graphical password types have been proposed in security. These graphical passwords are divided in three types as per the task to be performed in recollecting and entering the passwords- Recognition, Recall, and cued recall.

In recognition based password, visual objects are identified belonging to password portfolio. In this type, set of images are selected for login but there locations are changed. The user has to enter the correct selection. This process is repeated for every new login. Cumulative probability is calculated for successful login so to verify whether threshold exceeds the chances.

Recall based password to regenerate the interaction without cueing the sequence. The first recall based scheme in graphical password was Draw-A-Secret (DAS). The user draws the required password on 2D grid. Then the system encodes the sequence of drawing path along with grid cells.

Cued Recall password technique provides external cue which help user to memorize and enter password. In this type, user clicks the sequence of points on images as password and re-enter the sequence for authentication. Cued click points is similar to PassPoint but here only one image is used rather than multiple images.

2.2 Captcha

Captcha is used for differentiating between human and computers by using hard AI problems. There are two types of captcha schemes- Text Captcha and Image-Recognition Captcha (IRC). Text captcha works on character recognition whereas Image recognition captcha works on non-character recognition. Text captcha rely on difficulty of character segmentation which are complex and difficult to compute. Recognition of non-character object is more difficult than character recognition. IRCs rely on difficulty of object identifications or classifications. If both are combined together, difficulty of object segmentation is increased. IRCs are based on binary object classification or identification. Multi-label classification problems are much harder than binary object classification.

3. OVERVIEW

In CaRP, for the same user, a new image is randomly generated for every login attempt. CaRP uses alphanumerical characters, similar animals as well as special characters (alphabet of visual objects) to generate an captcha image, which will consider as a captcha challenge.

A major Difference between CaRP images and Captcha images is that user is allowed to input any password but not necessarily in a captcha image as all the visual objects in the alphabet should appear in a CaRP image.CaRP schemes are clicked-based graphical passwords. In case of memorizing the password and entering the same password while login, CaRP schemes can categories it into 2 methods: recognition and recognition-recall. Which needs recognition of an image and that recognized cues object image will be consider while entering a password. Recognition-recall is a new category where it is a combination of both recognition and cued-recall, and retains both the recognition-based advantage for human being to remember the password easily and the cued-recall advantage of a large password space.

Cued Recall password technique provides external cue which help user to memorize and enter password. In this type, user clicks the sequence of points on images as password and re-enter the sequence for authentication. Cued click points is similar to Pass Point but here only one image is used rather than multiple images.

4. RECOGNITION BASED CARP

In a CaRP scheme, a sequence of a visual object can be set as a password. As per traditional recognition based graphical passwords, it seems that this had an infinite number of visual objects to set as password pattern such as ClickText, ClickImage and ImageGrid. Among these patterns we are here implementing ClickText pattern and rest of 2 patterns can be generated in order to get more security to secure the password.

3.1 ClickText

ClickText is a recognition-based CaRP scheme which uses text Captcha as its underlying principle. Without any visually-confusing characters its alphabet comprises characters. For example, Letter "O" and digit "0" may be confusion in CaRP images, and thus one of these character either "0" or "O" should be excluded from the numeric value or alphabet respectively.

A password can be a sequence of a character in the alphabet, e.g., ρ ="AB#9CD87", which is same as a text password. Image for ClickText is generated by the underlying Captcha engine and all those confusing characters and numerics will be excluded from that generated image. These characters can be arranged randomly on 2D space. This is somehow different from text Captcha challenges where the characters are ordered from left to right for the users to type them sequentially. Fig. 1 shows a ClickText image with an alphabet of 33 characters [1].

Fig.1.A ClickText image with 33 characters [1].

3.2 ClickImage

Captcha Zoo [32] is a Captcha scheme which uses 3D models of horse and dog to generate 2D animals with different textures, colors, lightings and poses, and arranges them on a cluttered background. A user clicks all the horses in a challenge image to pass the test. Fig. 3 shows a sample challenge wherein all the horses are circled red [1].

ClickImage is a recognition-based CaRP scheme built on top of Captcha Zoo [32], with an alphabet of similar animals such as dog, horse, pig, etc. Its password is a sequence of animal names such as ρ = "Turkey, Cat, Horse, Dog," For each animal, one or more 3D models are built. The Captcha generation process is applied to generate ClickImage images: 3D models are used to generate 2D animals by applying different views, textures, colors, lightning effects, and optionally distortions. The resulting 2D animals are then arranged on a cluttered background such as grassland. Some animals may be occluded by other animals in the image, but their core parts are not occluded in order for humans to identify each of them. Fig. 2 shows a ClickImage image with an alphabet of 10 animals [1].

Fig. 2. A ClickImage image[1].

3.3 ImageGrid

The number of similar animals is much less than the number of available characters. ClickImage has a smaller alphabet, and thus a smaller password space, than ClickText. CaRP should have a sufficiently-large effective password space to resist human guessing attacks. ImageGrid's password space can be increased by combining it with a grid-based graphical password, with the grid depending on the size of the selected animal.

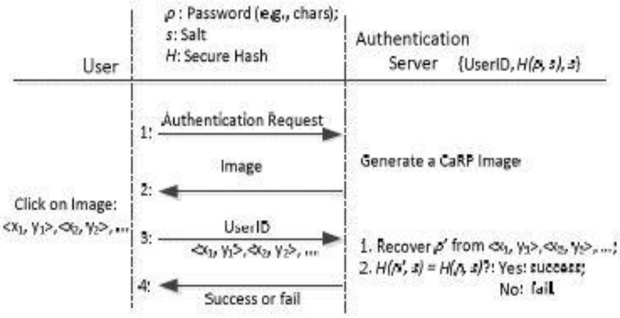
Fig. 3. A ClickImage image (left) and 6 × 6 grid (right) determined by
red turkey's bounding rectangle.

5. IMPLEMENTATION

ClickText CaRP was implemented using ASP.NET. web application framework. For ClickText configurable text Captcha was used which is commercially used by Microsoft. This Captcha system is designed in manner that it accepts only capital letters rejecting I, J, O, and Z ,and rejecting 0 and 1 from digits and "#", "@", and "&" these three special characters. The last three special characters were chosen to balance security and users'strong dislike of using non-alphanumeric characters in text passwords[3].Characters were rotated and scaled .The rotation range is -30° to +30° and the scaling range is 60% to 120% with neighboring characters overlapping up to 3 pixels.

CaRP scheme was implemented with a motive that it provides added security authentication server using Transport Layer Security (TLS).

Following mechanism is used for user authentication. For every user hash value H(p,s) is stored in authentication server (AS).The hash value contains salt s and password p. A CaRP password comprises of visual object or clickable points that user selects .Once login request is received AS server generates a CaRP image. This image is send to user to click the password. The co-ordinates of click points gets recorded and sent to authentication server along with ID credentials.AS works as follows. The received co-ordinates are mapped to CaRP image. A sequence of visual object Ids or clickable points are recovered as p'. AS then retrieves the salt of concerned account, hash value is then calculated with the salt. The result is compared with hash value stored in the database. Authentication is said to be successfully only if two hash value matches.



Flowchart of basic CaRP authentication[1]

6. SECURITY ANALYSIS

The simple captcha security analysis were case by case or on approximation based. There is no such theoretic security model yet established. A captcha challenge generally consist of 6-10 characters but in CaRP there are 30 or more characters. The complexity to break a Click-Text image is about α30 P(N)/(α10P(N)) = α20 times the complexity to break a CAPTCHA challenge generated by its underlying CAPTCHA scheme[1]. As CaRP system are arranged in two dimensions, segmentation becomes difficult and complex. Hence, it reduces distortion in generated images improving usability.

6.1 Online Guessing Attack

In automatic online guessing attacks, dictionaries are created manually by trial and error process. If negligible probability is ignored, object on one of the generated image are computationally-independent from another generated image in CaRP. Trials in guessing attacks are also mutually independent.

6.2 Human Guessing Attack

In human guessing attacks, passwords are entered by humans by trial and error process. Humans guessing process is much slower than computers. In simple captcha there are only 8 characters but in CaRP there are around 33 characters in ClickText which makes more complications for humans to track password. If we assume that 1000 people are employed to work 8 hours per day without any stop in a human guessing attack, and that each person takes 30 seconds to finish one trial. It would take them on average 0.5 · 338 · 30/ (3600 · 8 · 1000 · 365) ≈ 2007 years to break a ClickText password, 0.5 · 108 · 30/(3600 · 8 · 1000) ≈ 52 days to break ClickImage password, or 0.5 · 10 · 467 · 30/(3600 · 8 · 1000 · 365) ≈ 6219 years to break an ImageGrid password[1].

6.3 Relay Attack

Relay attacks are implemented in several ways. Considering captcha challenges on websites to be hacked, one way of attack is to have human surfers solve the challenges to continue surfing the Website [2]. The method used for solving CaRP is different from captcha challenge which makes person very difficult to crack the password. Even the input from user is useless for testing password guess in CaRP.

6.4 Shoulder-smurfing Attack

Shoulder-surfing attacks is generally observed when graphical passwords are entered in public place such as bank ATM. CaRP is not robust but combined with dual-view technology can be thwart shoulder-surfing attacks.

7. CONCLUSIONS

Captcha as Graphical password (CaRP) is new primitive security based on hard AI problems. CaRP is combination of captcha and graphical password scheme. CaRP technique mainly overcomes online guessing and human guessing attacks. In CaRP, image is generated using captcha challenge which is used for each login attempt. A password is set by user which is seen in generated image for login. In Recognition-based CaRP there are ClickText, ClickImage and ImageGrid technique. As CaRP does not rely on any specific captcha scheme, if one scheme is broken then new and more secured scheme is generated.

ACKNOWLEDGEMENT

We owe a great thanks to many people who helped and supported us during this project. Our deepest thanks to Prof. Stuti Ahuja, our project guide, for guiding & correcting several of our documents with attention and care. She has taken pain to go through the project and make necessary correction as and when required. We express our thanks to the Head Of Department (HOD), Prof. Leena Ladge for extending her co-operation and guidance throughout the project. Thanks and appreciation to our principal, Dr. Alka Mahajan for providing us with required facilities. We would also thank our classmates for their direct or indirect support for the project, without whom this project would have been a distant reality.

REFERENCES

[1] 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. IEEE TRANSACTIONS ON INFORMATION FORENSIS AND SECURITY, VOL.9, NO 6, June 2014

[2] Jayshree Ghorpade, Shamika Mukane, Devika Patil, Dhanashree Poal, Ritesh Prasad-" Novel Method for Graphical Passwords using CAPTCHA". International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-4 Issue-5, November 2014

[3] J. Bonneau, "The science of guessing: Analyzing an anonymized corpus of 70 million passwords," in *Proc. IEEE Symp. Security Privacy*, Jun. 2012, pp. 20–25.

[4] 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.

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

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