International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 08 | Aug 2018 www.irjet.net p-ISSN: 2395-0072

CaRP a graphical password: enhancing security using AI

Vipul Rana

UG Scholar, Computer Engineering Department, Shah and Anchor Kutchhi Engineering College, Mumbai, Mumbai University, Maharashtra, India

---

Abstract – *Security is one of the most important paradigm.It is yet not completely explored. Most of the security algorithms used presently works on mathematical formulas and AI problems. This paper describes a superintended method which is build on the Captcha method which is used almost everywhere on every website available on the internet. As a method to identify the user accessing the data is a human and not a machine. Captcha has become the approach used by all websites like social networking sites, banking systems, clouds. It is now almost a standard security step used to validate the user and secure the data from being abused by the bots. The new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks.*

Key Words: CaRP, Captcha, security primitive, algorithm, guessing attack, relay attack.

1. INTRODUCTION

The most important job in security is to create cryptographic methods using mathematical problems which are computationally intractable. We can take the example of the integer factorization which is fundamental to the RSA public key cryptosystem. The idea of using hard AI problems for security which were proposed in [2], is an exciting new pattern. Under this pattern, one of the primal method brought into action is the Captcha, which identifies the human users and the bots by giving challenges like puzzles which are possible to solved by the humans but above the capability of the systems. It is now a standard security technique used to protect the integrity of the data. Captcha works on the gap of potential between the humans and the systems for solving certain AI problems. The captcha can be differentiated in two type: text Captcha and Image Recognition Captcha (IRC).

1.1 Captcha as a part of Authentication

It was first used in [3] to use both the methods i.e. the Captcha and the passwords as a requirement for the purpose of authentication of a user which is called as Captcha-based Password Authentication (CbPA) protocol. The CbPA protocol can be termed as two step authentication protocol. In this protocol the user firstly uses his credentials i.e. username, password and then the user is been displayed a captcha which he needs to identify to prove that the attempt made for the access is requested by the actual human user not any system. A specific threshold value is been set for login attempts. Which limits the attempts of the unknown systems from attempting then from using malicious attacks and spywares [4][5]. Captcha is located below the pass-image the user has to recognize the pass-image and enter the text from the image as a step included in authentication of the user.

1.2 Captcha as graphical passwords

It is a new way to thwart guessing attacks. Speaking of guessing attacks lets see how the attack works. In this attack ,a password is guessed in a successful trial is determined wrong and excluded from the subsequent trials. The number of the undetermined guess of password decreases with the increase in the trial of the passwords. Which may help giving open chance to find the password.

Mathematically, lets 'S' be the number of the password guess before the password trial and error is performed. We will be denoting 'p 'as password and 'T' represents the trial. 'Tn' denotes the number of the trial and p(T=p) be probability of p tested in the trial. 'En' be the password guesses tested up to Tn. giving the Equation:

$$p\,(T = \rho | T1 \_= \rho, \ldots, Tn-1 \_= \rho) > p(T = \rho), \quad (1)$$

and

$$En \rightarrow S$$

$$p(T = \rho | T1 \_= \rho, \ldots, Tn-1 \_= \rho) \rightarrow 1\} \text{with } n \rightarrow |S|, \quad (2)$$

where $|S|$ denotes the cardinality of S. From Eq. (2), The password is always achieved within the |S| trials, if the password is in the S. Otherwise it is terminated. There are lots of approaches to counter the guessing attack but no matter what it can always be cracked by the brute force attack.

But CaRP uses completely different method to counter these attacks. It uses the equation mentioned below which states that each and every trial is independent of each other.

$$p(T = \rho | T1, \ldots, Tn-1) = p(T = \rho), \forall n$$

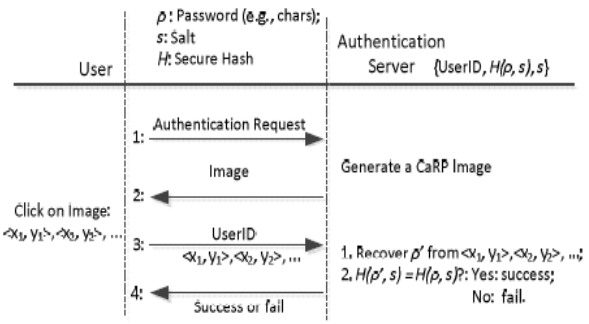
The idea to counter those attack is the image shown for the authentication is different for each trials. So the guessing

attack fails as the trials fails the image also changes so it can't be guessed. This capability gap between humans and machines can be taken advantage of to generate images so that they are computationally independent yet retain properties that only humans can identify, and thus use as passwords. The invariants among images must be intractable to machines to thwart automatic guessing attacks.

2. CaRP: An Overview

In CaRP for every attempt of login a new image is generated for user. CaRP uses images of characters, alphabets, group of similar animals, etc. Many CaRP are generated using Captcha scheme. CaRP are click based graphical passwords. The principle of converting a captcha into CaRP states any Captcha scheme have two or more recognizable predefined objects can be converted. The CaRP scheme must ensure two most important factor security and usability. Security from the system and the attacker and usability by the user should not be much complicated. This scheme is used with additional protection with the help of Transport Layer Security(TLS) channel

Fig 1: Flowchart of basic CaRP Authentication



2.1. CaRP: Types

The schemes of CaRP are graphical password based on clicks. The CaRP schemes can be differentiated in two types: Recognition and Recognition-Recall which requires recognition of an image and those objects as the links to the password. Recognition-Recall can be called as a mixture of both the recognition and the cued-recall system.

2.1.1 Recognition Based CaRP

The Recognition based CaRP views password as the visual objects in the sequence. Recognition-based CaRP have access to an infinite number of different visual objects.

The different variations of Recognition based Carp are:

- Click Text
- Click Animal
- Click Grid

2.1.2 Recognition-Recall CaRP

It is a recognition of password which is a invariant pattern of objects. An invariant point of an object is the point that has the relative position of the point with different font which still can be understood by human irrespect of the CaRP image. The user has to identify the password displayed on the screen and based on that the user has to track the cues and locate the position matching the given password. Fixed number of correct answers are required by the user [6].

The different types of Recognition-Recall CaRP are:

- TextPoints
- TextPoints4CR

3. CONCLUSIONS

The paper highlights a new security primitive known as CaRP. CaRP is a combination of both Captcha and a graphical password scheme. This approach helps us to keep our data secure from the bots and other online attacks. CaRP is similar to Captcha security but in CaRP every attempt is individual as per the CaRP for every attempt different challenge is given. So this makes the CaRP a safe and secure way of protecting our data from online guessing attack, brute force attack, etc. So using the hard AI problems we can use CaRP as a step towards the security. As CaRP fits in the gap between the humans and the understanding of the systems. It makes CaRP much more efficient from the security point of view.

REFERENCES

[1] Bin B. Jhu, Jeff Yan, Guanbo Bao, Maowei Yang and Ning Xu: "Captcha as a Graphical Password-A new Security Primitive Based on Hard AI Problems" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE 2014

[2] 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.

[3] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in Proc. ACM CCS, 2002,pp.161170.

[4] 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.

[5] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "Against spyware using CAPTCHA in graphical password scheme," in Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl., Jun. 2010, pp. 1–9.

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

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

[9] 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.