2nd National Conference on Recent Innovation in Engineering, Science, Humanities and Management
REVA University, Yelahanka, Bangalore, (India)
29th-30th March 2019 www.conferenceworld.in ISBN : 978-93-87793-79-8

Captcha As Graphical Passwords – A New Security Based On Hard AI Problems

Nivedha.A, Sheetalsingh.B, Rohitha , Bhimamma
Prof.Natraj Urs HD
Asst.Prof., School of ECE

ABSTRACT

Nowadays, authentication is one of the important fields in information security. Strong text-based password could provide certain degree of security level. However, the fact that, those strong passwords are difficult to memorize by the users. Graphical authentication has been proposed as an alternative solution to text-based authentication. Many researches shows that humans can remember images better than text. In recent years, many networks, computer systems and Internet based environments used graphical authentication technique for authentication. But this graphical authentication technique has many limitations. CAPTCHA is a programme that protects website against bots by generating and grading tests that human can pass but current computer program cannot. This paper present a new technology called Captcha as graphical Password (CaRP). CaRP combines both CAPTCHA and graphical password scheme. CaRP offers protection against dictionary attacks, relay attacks, shoulder surfing attacks.

Keywords: Graphical password, CaRP, Captcha, dictionary attack, password guessing attack, protection primitive.

INTRODUCTION

Graphical password techniques are an alternative to alphanumeric passwords in which users click on images to authenticate themselves rather than using alphanumeric strings. Because of increasing threats or misuses to networked computer systems there is great need for security innovations system. Security practitioners and researchers have made stalk in protecting systems and individual users' digital assets or sensitive data. Users interact with security technologies either passively or actively. For passive use, users must have understood ability. For active use people must need much more from their security solutions: ease of use, memorability, efficiency, effectiveness and satisfaction.

Authentication is the mechanism of determining whether each user should be allowed access to a particular system or resource. It is a critical area in the field of security research and practice. Alphanumeric passwords are used widely for authentication purpose, but other methods are also available, including biometrics and smart cards for authentication. Many problems that the users have with alphanumeric passwords which are mainly related to memorability of secure passwords or strong password. In an attempt to create more memorable passwords that helps the users, graphical password systems have been invented. In these systems authentication is based on clicking over images rather than typing alphanumeric strings. Several kinds of graphical passwords have been invented.

A graphical password scheme is an authentication system that works by having the user select click points from images, in a specific order, which is presented in a graphical user interface (GUI) to the user. The graphical-password approach is also called graphical user

authentication (GUA).A graphical password is easy to memorize than a text-based password for most people. Suppose an minimum of 8-character password is necessary to gain entry into a particular computer network. Instead of w8KiJ72c, a user might select images of the earth the country of France, a white stucco house with arched doorways and red tiles on the roof and so on.

The proposed system introduce a new security primitive based on hard AI problems, namely, a novel family of graphical password systems integrating Captcha technology, which called as CaRP (Captcha as graphical Passwords). CaRP is both a Captcha and a graphical password scheme.A CAPTCHA is a program that protects websites against automated actions by generating tests that humans can pass easily but computer programs cannot. The term CAPTCHA (for Completely Automated Public Turing Test To Tell Computers and Humans Apart) was invent in 2000 by Luis von Ahn, Manuel Blum, Nicholas Hopper and John Langford of Carnegie Mellon UniversityCaRP is click-based graphical passwords, where a sequence of clicks points on an image is used to create a password. Unlike other click-based graphical passwords schemes, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every user's login attempt. CaRP offers protection against online dictionary attacks in the field of web application, which have been for long time a major security threat for various online web services. CaRP also offers protection against relay attacks, an increasing security threat to bypass Captchas protection, where in Captcha challenges are easy to humans to solve. CaRP requires solving a Captcha challenge in every user's login.

METHODOLOGY

A new user initially registers to the system by providing username, email, phone number, CaRP password Text based allow user to enter text based, which is minimum of six[6,7] alphanumeric strings. Next level is CaRP where user needs to click correct image specified by the system.Each login or registration time the images are displayedin random sequence.

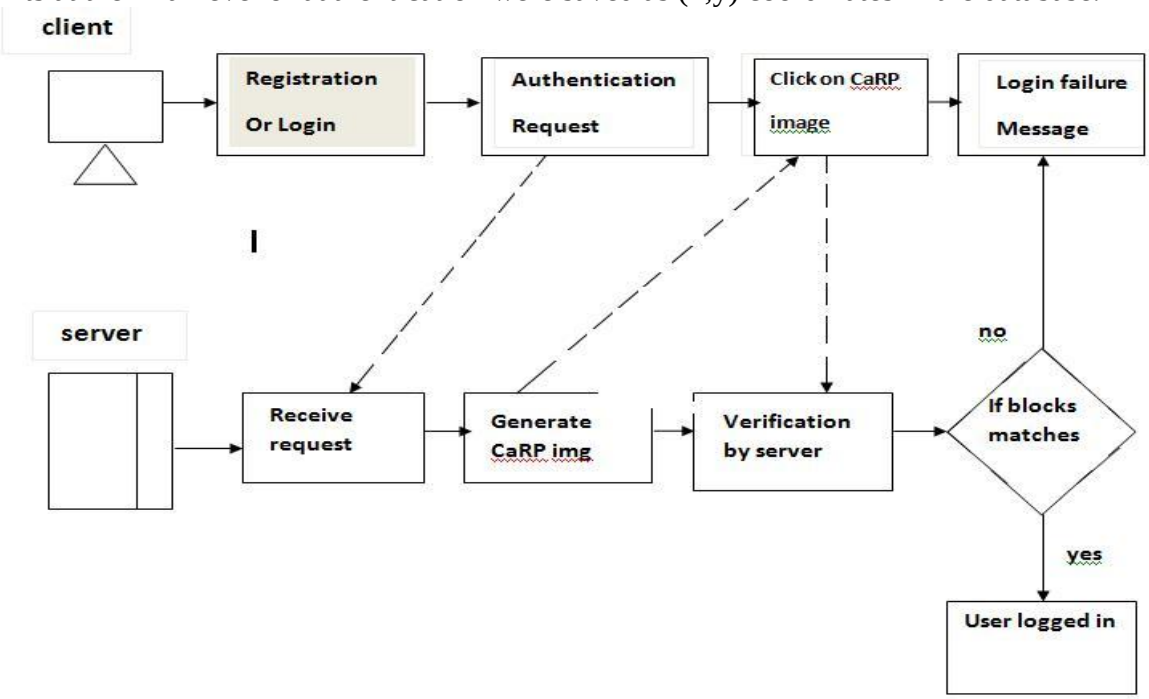
In CaRP password selection, a set of animal image are stored in the database. On registeration these stored animal images are displayed in grid form to the user interface randomly. Also the name of the images as in text form shows randomly to each user. Each user at registration time need to select the corresponding animal image as per the displayed text(name of the animal).This image will be the user CaRP password.
User need to memorize this selected image for authentication. This correct selection can be done only by a human. While the bots feel this as a difficult task. Hence this reduces automated attacks made by the attackers. If the selection is right, then user need to select click point password.

Here user need to click some points(three points) on the selected image as their password. This scheme is flexible to the user because it allows any image to be used, e.g. natural images, paintings, etc. The images could be chosen by the user. The only practical requirement is that the image be intricate and rich enough so that many possible click points are available.

Another flexibility is that do not need artificial predefined click regions with marked boundaries. A user's password consists of any randomly chosen sequence of points in the image. Since an tangled image easily has hundreds of memorable points, not many click points are needed to make a password hard to guess. For example, with five or six click points one can make more passwords than 8-character Unix-style alphanumeric passwords over a standard 64-character alphabet. The authentication process involves the user selecting several points on picture in a particular order.

When logging in, the user is supposed to click close to the selected click points, within some (adjustable) tolerance distance. Here only one image is needed for the user to set their password in this level. At authentication time, user need to provide username, email, text password, CaRP image password and click points password. If this selction is right, then login success. Then the user enter to their own accounts. Each user can store documents to their accounts.

The systems provide an option for setting security to the stored documents. For security reasons, the system should not store passwords explicitly. User's text password, click points were saved in encrypted format using AES-128 encryption algorithm. Advanced Encryption Standard (AES) algorithm is not only for security but also for great speed. The user clicked points at the final level of authentication were saved as (x,y) coordinates in the database.



CONCLUSION

Here proposed CaRP, a new protection primitive relying on unsolved hard AI problems. The notion of CaRP presents a fresh class of graphical passwords, which adopts a fresh approach to stand online estimating attacks: a new CaRP image, which is too a Captcha task, is used for every login shot to make trials an online estimating attack computationally individual of

each other. A password of CaRP can be start only probabilistically by unthinking online guessing attacks counting brute-force attacks, a desired protection property that other graphical password systems lack. In addition to proffering protection from online guessing attacks, CaRP is also immune to Captcha relay attacks, and, if pooled with dual-view technologies. CaRP can also help cut down spam dispatches sent from aNet email facility.

Acknowledgements

We owe a great thanks to many people who helped and supported us during this project. Our deepest thanks to Ast Prof. NatrajUrs H,D., our project guide, for guiding & correcting several of our documents with attention and care. He has taken pain to go through the project and make necessary correction as and when required.

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

Journal papers

[1] JayshreeGhorpade, ShamikaMukane, DevikaPatil, DhanashreePoal, 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

[2] Bin B.Zhu, Jeff Yan, GuanboBao, Maowei Yang, and NingXu. 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

[3] 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.

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

[5] HosseinNejati, Ngai-man Cheung, Ricardo Sosa and Dawn C.I.Koh.DeepCaptcha: An Image CAPTCHA Based on Depth Perception. ACM digital Library, March 2014.

[6] P.R.DevaleShrikala, M. Deshmukh and Anil B.Pawar. Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme. International Journal of Soft Computing and Engineering, Volume-3, Issue-2 May 2013