CaRP Using Discrete Centralization Methods

Sudarshan Pawar
UG Student
Singhad Academy of Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India

Snehal Katare
UG Student
Singhad Academy of Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India

Varsha Jethwani
UG Student
Singhad Academy of Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India

Topaz Arengh
UG Student
Singhad Academy of Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India

Shalini Wankhade
Professor
Singhad Academy of Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India

Abstract

Information Security has always been like cat & mouse . To be precise, attackers are always hunting for weaker targets & develop more advanced tools to exploit the networks as well as humans i.e. attacking e-mail accounts, Social Networking Sites etc. Many I.T. Industries have stood against these attackers & succeeded in blocking most of their attacks by introducing CAPTCHA. Still there is no foolproof solution for these attacks. Taking in consideration for security against Email Accounts, it is possible that attacks viz. Dictionary Attacks, Brute-Force Attacks and Shoulder Surfing lead to successful exploitation. So, we introduce new method CAPTCHA as Graphical Passwords (CaRP) that eliminates all possible attacks against the attacks mentioned above using various password schemes. Evolving from CAPTCHA technology, this method i.e. CaRP uses graphical implementations as a password for the user, thus making the user to click on certain click points in order to submit his/her password successfully.

Keywords: CAPTCHA, Dictionary Attacks, Graphical Passwords, Brute-Force Attack, Password Schemes, Click Points.

I. INTRODUCTION

We have seen CAPTCHA needed to be computed/solved by the authenticate user in order to perform a successful login into any email service. So, CAPTCHA was considered to be a security measure that could stop bots to login. But, there some tools like 'Tessercap' that performs successful attack on any CAPTCHA. After this we can now say that having static CAPTCHA is not a foolproof security measure. To solve this issue we have seen animated CAPTCHA which is complicated to attack & be successful. So, a new technique where CAPTCHA is itself a password is described in the following paper.

II. SECURITY ISSUES

A. Keyloggers

Keyloggers are the tools that monitor the system of a user/target & records all keystroke entered while the machine is in use.This tool is made undetectable by antivirus programs, & sometimes attackers bind this tool to some port of the user & record all keystrokes remotely

B. Brute-Force & Dictionary Attacks:

These type of attacks are performed on regular string based passwords. These tools use Rainbow Tables & a Dictionary as the brute-force input. But this can be blocked by introducing Captcha solving by the user.

C. Tessercap[3]:

TesserCap is a simple CAPTCHA solving tool that can be used to test CAPTCHA images. TesserCap is a GUI-based, highly flexible, point-and-shoot CAPTCHA analysis tool with the following features:

(1) A generic image preprocessing engine that can be configured as per the CAPTCHA type being analyzed.
(2) Tesseract as its OCR engine to retrieve text from preprocessed CAPTCHAs
(3) Web proxy and custom HTTP headers support
(4) CAPTCHA statistical analysis support
(5) Character set selection for the OCR engine.

III. CARP METHODS

A. ClickText Based[1]:

The graphical captcha in this method based on characters i.e.A-Z|a-z & 0-9. Here, the user clicks on the particular character(alphabet or number) at a specific point registered or to register the password. Fig 1 Simplifies shows all characters displayed to user while entering his/her password. To add more security, one could also select the some region of the character image (Fig.2 Textpoints) for assigning his/her password.

Fig. 1: Text Characters

Fig. 2: Text Points

B. Select Object Based[1]:

Here in Fig. 4,the user is requested to select an image among all images displayed in the grid. If the user has assigned an object from the grid, on next login he/she needs to select that same object to get successful login.

Fig. 3: Object Selection In A Grid

C. Grid Based[1]:

The user is asked to click on specific point on an images registered previously.

Image1

1	16	12	21	28	30
4	20	27	32	18	7
10	5	2	22	15	29
3	23	13	34	11	31
14	26	19	6	25	35
17	9	24	33	36	8

Image2

Here, Image 1 is displayed first to the user. He need to click on specific region(i.e. (x,y)co-ordinate) registered in-order to obtain the grid having numbers in 6x6 table. Any click outside authenticate region would be considered as incorrect password. The password is stored in following manner: (x,y,number in the grid) ex.(45,12,36) where 45,12 is the x,y co-ordinate & 36 is static co-ordinate & password number respectively to be provided.[Note: Grids displayed on Image 1 are for representation only. The user will not see any grid marking or other attributes stating the specific authenticate region.

IV. DISCRETE CENTRALIZATION USAGE

Discrete centralization [5] is used to rectify the errors caused in the tolerance region. If there is a static grid created, then there might be a situation where the click point is between two regions whose co-ordinates vary. This results in incorrect password. So, generating the co-ordinates dynamically evenly across the image solves this problem.This dynamic generation of (x,y) co-ordinates is done by centralization.

V. CONCLUSION

(1) CaRP can block Dictionary & Brute Force Attacks

(2) It also secures accounts by blocking attacking on Captcha itself.
(3) Usage of CaRP can be time consuming.

REFERENCES

[1] Captcha as Graphical Passwords—A New Security_Sonia Chiasson (Carleton University), Jayakumar Srinivasan(Toronto, Canada),Robert Biddle(Carleton University),P. C. van Oorschot(Carleton University)
[2] Captcha as Graphical Passwords:A new Security Primitive Based on Hard AI Problems_Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, & Ning Xu
[3] Attacking Captcha for fun & profit_ Gursev Singh Kalra, Managing Consultant, McAfee® Foundstone® Professional Services
[4] Graphical Password Authentication Using Cued Click Points_Sonia Chiasson, P.C. van Oorschot, and Robert Biddle
[5] Centered Discretization with Application to Graphical Passwords (full paper)_ Sonia Chiasson (Carleton University), Jayakumar Srinivasan(Toronto, Canada),Robert Biddle(Carleton University),P. C. van Oorschot(Carleton University)
[6] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better passwords: Persuasive cued click-points," in *Proc. Brit. HCI Group Annu. Conf. People Comput., Culture, Creativity,Interaction*, vol. 1. 2008, pp. 121–130.
[7] Yan and A. S. El Ahmad, "A low-cost attack on a Microsoft CAPTCHA," in *Proc. ACM CCS*, 2008, pp. 543–554.
[8] G. Moy, N. Jones, C. Harkless, and R. Potter, "Distortion estimation techniques in solving visual CAPTCHAs," in *Proc. IEEE Computet. Society.*
[9] John the Ripper Password Cracker [Online]. Available: http://www.openwall.com/john/, http://openwall.info/wiki/john/tutorials
[10] THC HYDRA Tool, Available in Kali Linux. [Online] http://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-online-passwords-with-tamper-data-thc-hydra-0155374/