A New Security Primitive Model Based on Artificial Intelligence Using Captcha as Graphical Passwords

Sandeep H 1, Dr.B K Raghavendra 2

1Assistant Professor, Department of Computer science and Engineering, KSSEM, Bengaluru, India
2Professor and Head, Department of Computer science and Engineering, KSSEM, Bengaluru, India

ABSTRACT:

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. Notably, a CaRP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. CaRP also offers a novel approach to address the well-known image hotspot problem in popular graphical password systems, such as Pass Points, that often leads to weak password choices. CaRP is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security.

Keywords: Captcha as Graphical Password (CaRP), Security Primitives, Online Security.

[1] INTRODUCTION

Image processing is a method to convert an image into digital form and perform some operations on it, in order to get an enhanced image or to extract some useful information from it. This is a type of signal dispensation in which input is image, like video frame or photograph and output may be image or characteristics associated with that image. Usually Image Processing system includes treating images as two dimensional signals while applying set of signal processing to them. These are among rapidly growing technologies today, with its applications in various aspects of a business. Image Processing forms core research area within engineering and computer science disciplines. The two types of methods used for Image Processing are Analog and Digital Image Processing. Analog or visual techniques of...
image processing can be used for the hard copies like printouts and photographs. Image analysts use various fundamentals of interpretation while using these visual techniques. The image processing is not just confined to area that has to be studied but on knowledge of analyst. Association is another important tool in image processing through visual techniques. So analysts apply a combination of personal knowledge and collateral data to image processing.

Digital Processing techniques help in manipulation of the digital images by using computers, as raw data from imaging sensors from satellite platform contains deficiencies. To get over such flaws and to get originality of information, it has to undergo various phases of

[2] METHODOLOGY

The presented new security primitive based on 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. Notably, a CaRP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set.

CaRP also offers a novel approach to address the well-known image hotspot problem in popular graphical password systems, such as Pass Points, that often leads to weak password choices. CaRP is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security.

Exemplary CaRPs built on both text Captcha and image-recognition Captcha are also presented. One of them is a text CaRP wherein a password is a sequence of characters like a text password, but entered by clicking the right character sequence on CaRP images. CaRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services. This threat is widespread and considered as a top cyber security risk. Defense against online dictionary attacks is a more subtle problem than it might appear.

[3] AGORITHMS

**Captcha Graphical Password Setting**

Once Admin create a user account, a link address is emailed to valid user. By clicking the link, user can generate the Captcha Graphical Password Code.

**Process involved in Captcha Graphical Password Code Generation**

1. Pick randomly nine images from the image db.
2. Merge the nine images into single Captcha.
3. Display the Captcha to the user.
4. Initialize String S
5. User has to pick any one image and click a point in the image
6. Using Coordinate system find the click coordinate
7. Append the Image Code + Click coordinate to $S$
8. Ask User “Whether he need to add more Images?” and get the response
9. If response is Yes GOTO step 5
   Generate Captcha Graphical Password Code (PASSCODE) using Hashing Technique on String $S$.
10. Store the PASSCODE in User’s Record.

Captcha Graphical Password Verification

When user trying to enter into his home page this process will take place.

Process involved in Captcha Graphical Password Code Verification
1. Pick the $N$ images which are selected by user in Code Generation Process.
2. Pick randomly $9-N$ images from the image db.
3. Merge the nine images into single Captcha.
4. Display the Captcha to the user.
5. Initialize String $S$
6. User has to pick any one image and click a point in the image
7. Using Coordinate system find the click coordinate
8. Append the Image Code + Click coordinate to $S$
9. Ask User “Whether You need to Click more Images?” and get the response
10. If response is Yes GOTO step 5
    Generate Captcha Graphical Password Code PASSCODE1 using Hashing Technique on String $S$.
11. Retrieve the PASSCODE which is Stored User’s Record.
12. If PASSCODE = PASSCODE1 then verification success, Allow the user to Home Page Else Verification Failed, Show the Message to user.
RESULTS

Fig 4.1 : The Admin Login page

The fig 4.1 shows the admin login page. Admin will login and also have the permission to edit his own profile. Admin can see the account details of user and perform the access on that module and send mail to user which contains account holder information with captcha graphical password links, and admin can have all the branch details and he can change his own password to access the particular module.

Fig 4.2 Adding Account of user by admin
The above fig 4.2 shows the login page of the admin where it contains account type, account details, branch details, change password and log out.

Fig 4.3 setting of graphical password from the sent link.

The fig 4.3 shows the Captcha image. It is the image consisting of 9 images combined together from which the user is allowed to select his desired point for which the code is generated.

Fig 4.4 Transfer Beneficiary Account Details
The fig 4.4 shows the page for transferring beneficiary account details using which the transfer of amount can be done. The user can transfer the amount which is protected via messages.

Fig 4.5 URN no message to confirm the Beneficiary

The fig 4.5 shows the URN number sent to the mobile number which is given during the creation of account. This URN number is used to confirm the Beneficiary.

[6] CONCLUSION

The proposed CaRP, a new security primitive relying on unsolved AI problems. CaRP is both a Captcha and a graphical password scheme. The notion of CaRP introduces a new family of graphical passwords, which adopts a new approach to counter online guessing attacks, a new CaRP image, which is also a Captcha challenge, is used for every login attempt to make trials of an online guessing attack computationally independent of each other. This work is one step forward in the paradigm of using AI problems for security. CaRP has good potential for refinements, which call for useful future work.

REFERENCES

[1] Intelligence Problems”, Bin Benjamin Zhu, Guanbo Bao, Maowei Yang, Ning Xu.


Author brief Introduction

1. Sandeep H
   Assistant professor, Dept. of CS&E

2. Dr. B K Raghavendra
   Professor and Head, Dept. of CS&E

Corresponding Address-
K.S. School of Engineering and Management
Off., 15, Kanakapura Rd, Talaghattapura, Bengaluru, Karnataka 560109