A New Security Primitive using Captcha as a Graphical Password

Dahake Shashank1 Gund Rahul2 Vichare Akshay3 Gavhane Yogesh4

1,2,3,4 Dhole Patil College of Engineering Wagholi, Pune

Abstract— Depends on hard mathematical problems there are many security primitives. But there are many new paradigm, that are still has been underexplored. In this paper based on hard AI problems we present a new security primitive, on top of Captcha technology a novel family of graphical password systems built, which we call Captcha as graphical passwords (CaRP). CaRP can be used as a graphical and Captcha scheme. CaRP has a number of security problems generally it come with online guessing attacks, relay attacks, and if combined with dual-view technologies, shoulder-surfing attacks. Here we can notice one thing that in automatic online guessing attacks CaRP password can be found only in probabilistically even if the password is in the search set. To address the well-known image hotspot problems in popular graphical password system CaRP also offer a novel approach, such as Pass Points, which often leads to weak password choices, CaRP is not panacea, but it offer reasonable security and usability and for improving online security appears to fit well with some practical application.

Key words: Captcha, dictionary, attack, graphical password, security, password guessing, attack

I. INTRODUCTION

To create cryptographic primitives based on hard mathematical problems that are computationally intractable, a fundamental task in security. For example, to the-RSA public-key cryptosystem and the Rabin encryption the problem of integer factorization is fundamental. In the some of the existing system diffie Hellman key exchange have been used.

The new paradigm is, Using hard AI (Artificial Intelligence) problems for security, initially proposed in [13]. Distinguishes human users from computers

Under this paradigm, by the most notable primitive invented is Captcha, by presenting a challenge, i.e., captcha is the challenge for the computer but easy for the human being to solve the problem. To protect online email and other services from being abused by bots Captcha is now a standard Internet security technique. Even this paradigm is achieved with somewhat limitations in the hard mathematical problems. . The main challenge is to find it is easy to get the solution for the problem based on hard AI. The Captcha is the challenging problem in AI.

We introduce a new security primitive based on hard AI problem. In this paper we have used CaRP where sequence of clicked points on the graphical image is used to derive a password. The image used in the captcha is the captcha challenge generated for every login attempt unlike other click-based graphical passwords. The notion of CaRP is generic and simple. In the existing methods the CaRP scheme on both texts Captcha and image-recognition Captcha We present exemplary CaRPs built. In the text based password system keywords are used as a password. Sequence of characters like a text password, but entered by clicking the right character sequence on CaRP images. Against online dictionary attacks on passwords CaRP offers protection, which has been for long time a major security threat for various online services. This threat is widespread and considered as a top cyber security risk [13] a more subtle problem than it might appear is Defense against online dictionary attacks. Intuitive countermeasures such as throttling logon attempts do not work well for two reasons:

1) It causes incurs expensive helpdesk costs for account reactivation and denial-of-service attacks (which were exploited to lock highest bidders out in final minutes of eBay auctions [12]).

2) Adversaries intend to break into any account rather than a specific one by It is vulnerable to global password attacks [14], and thus to avoid triggering account lockout, try each password candidate on multiple accounts and ensure that the number of trials on each account is below the threshold.

Against relay attacks, CaRP also offers protection, an increasing threat to bypass Captcha protection, wherein Captcha challenges are relayed to humans to solve. To bypass Facebook’s Captcha in creating new accounts Koobface [16] was a relay attack, if combined with dual-view technologies CaRP is robust to shoulder-surfing attacks.

CaRP requires solving a Captcha challenge in every login by adapting the CaRP image’s difficulty level based on the login history of the account and the machine used to log in This impact on usability can be mitigated.

Typical application scenarios for CaRP include:

1) On typing passwords is cumbersome, esp., CaRP can be applied on touch-screen devices. for secure Internet applications such as e-banks. Many e-banking systems have applied Captchas in user logins. For example, ICBC (www.icbc.com.cn), the largest bank in the world, requires solving a Captcha challenge for every online login attempt.

2) CaRP increases spammer’s operating cost and thus a spam but cannot log into an email account even if it knows the password For an email service provider that deploys CaRP. Instead, human involvement is compulsory to access an account. To throttle the number of emails sent to new recipients per login session If CaRP is combined with a policy, before asking human assistance for login, leading to reduced outbound spam traffic a spam both can send only a limited number of emails.

The remaining paper is organized as the section II describe the existing methods of the security in the literature survey, section III describe the proposed work section IV conclude the proposed work and future enhancement in the proposed work.

II. LITERATURE SURVEY

Till the date large number of password has been proposed. These methods are classified into three main classes as
follow. Reorganization, recall, and cued click point. In the recognition based system decoys the visual object related to the password portfolio. In this scheme the faces are given to the user. The process is repeated for the several time and each time with differential panel user need to select the face. To do the successful login to the system it required selection of same points each time. For the every round the set of images are remains same but the location of the image get changed. The method used in [17] is also same as discussed above but the image generated in this system is large in number. In the recall based method user generate same interaction result without cueing. The first recall method is draw a secrete (DAS)[3]. In this method user draws her password on a 2D grid. The system encodes the sequence of grid cells along the drawing path as a user drawn password. The next method is Pass-Go [4] can improves DAS’s usability by using the encoding the grid intersection points rather than the grid cells. The next method is BDAS [20] which adds background images to DAS to encourage users to create more complex passwords than old methods. The third method is the cued click point in which the cued points are added for the memorization and passwords. The pass based scheme described in [5] is the more suitable scheme for the cued click point. The user can click the point on the image randomly and same points must have to click at the time of login.

Among this three schemes Reorganization scheme is best for the human being because human being can recognize very well while pure recall is tough to the human being.

Captcha is nothing but the gap of the capabilities between human being and bots in the solving the hard AI problem. In general there are two types of captcha are there one is the text captcha and second is the image captcha. Textual captcha is depend on the segmentation of the textual images.

III. PROPOSED SYSTEM

In the proposed system we have used captcha as a graphical password. For the proposed system password is the sequence of selected virtual objects. CaRP have access to the infinite numbers of visual objects.

A. Clicked Text:

Clicked text is the reorganization based captcha generally coming under the text captcha. Its alphabets consist of the characters without any confusing characters. For example the number 1 and small character L can make confusion so we have removed such a characters. The text password is the collection of the sequence of clicked characters which is similar to the text password. In the clicked image characters can be added randomly in the different format. The combination of the characters is shown in the following figure.

Fig. 1: Clicked Text

The above figure consist of the 33 different characters user need to click different characters this characters will be set as a password for the particular user. In the above figure the sequence of characters selected are placed in the database and this characters are retrieve at the time of the login to the particular system

B. Clicked Image:

In this type of the captcha user will click on the different position on the image. The x and y coordinators of the image is stored in the database. in the existing system such as click animal the animal name are stored in the database such as horse, donkey, monkey etc. but in the proposed system we are working on the x and y coordinators of the image. For example as shown in the following figure if user first clicked on the left eye of the image it will store its X and Y coordinates value in the database. Here no any concern of the image is combination of different images or it is a single image. It will store value such as AP (150,170), where 150 is the value of X coordinator and 170 is the value of the Y coordinator respectively. Password is sequence of the clickable points. For example in the following figure user clicked on different points of the image then this points are stored in the database with sequence.

Fig. 2: Image Clicked Point

IV. ALGORITHM USED

A. Virtual Keyboard Algorithm:

To provide the security against the shoulder surfing attack we are using virtual keyboard algorithm. In which the layout
of the keyboard get changed after pressing every word in the password. There are following steps in this algorithm,

1) Initialize the all keyboard buttons in the QWERTY pattern.

2) While the key is pressed,
   - Stored all numbers and alphabets in the array.
   - Randomize the all alphabets and numbers in the array.
   - Reassign the newly formed alphabets and numbers to the buttons in the array.
   - Display the characters on the buttons.
   - if enter key is pressed g

3) Check the length of the keys entered in the database.
   - If (length = valid)
4) Check for the password match.
   - If password matches go to step 6.
   - Else go to step 5.
5) Second level of authentication
6) End.
7) end if
8) end for
9) along the text stroke Boundaries after the document
10) Then new binary result Store to B f

V. SECURITY ANALYSIS

Computational intractability in recognizing objects in CaRP images is fundamental to CaRP. Existing analyses on Captcha security were mostly case by case or used an approximate process. No theoretic security model has been established yet. Object segmentation is considered as a computationally expensive. Click Animal or image relies on both object segmentation and multiple-label classification. Its security remains an open question. As a framework of graphical passwords, CaRP does not insure on any specific Captcha scheme. If one Captcha scheme gets broken, a new and more robust Captcha scheme may appear and be used to construct a new CaRP scheme. In the remaining security analysis, we assume that it is intractable for computers to recognize any objects in any challenge image generated by captcha. In automatic online guessing attacks, the trial and error process is executed and the dictionary is created. The third attack is the relay attack this attack can be executed by several ways, the capTCHA can overcome this attack. The fourth attack is the shoulder surfing attack. This attack can be get in the public place. The shoulder surfing attack can be found in the public place. CaRP can reduce the risk of the shoulder surfing attack.

VI. CONCLUSION

We can conclude that we have proposed CaRP a novel method to overcome the problems of the security attacks such as shoulder surfing, online password guessing attacks, relay attacks etc. In CaRP we have used captcha and also graphical password. CaRP introduces the notion of the graphical password which reduces the risk of online password guessing attack. In this we have proposed new approach which can change the arrangement of the keyword at each login attempt. The proposed system reduces the shoulder surfing attack by using virtual keyboard because every time the layout of the keyboard get changed. our work is one step forward in the paradigm of using hard AI problems for security. Of reasonable security and usability and practical applications, CaRP has good potential for refinements, which call for useful future work. More importantly, we expect CaRP to inspire new inventions of such AI based security primitives.

VII. ACKNOWLEDGMENT

We would like to take this convenience to explicit our deep obligation and deep view to our Project Guide (name), for his excellent advice, beneficial feedback and constant confidence throughout the duration of the project. His beneficial suggestions were of enormous help throughout my project work. His discreet criticism kept us working to make this project in a much better way. Working under him was an extremely appreciative experience for us.

REFERENCES

[6] ZHU et al.: NEW SECURITY PRIMITIVE BASEON HARD AI PROBLEMS 903
A New Security Primitive using Captcha as a Graphical Password


(20) S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, “Influencing users towards better passwords: Persuasive cued click-points,” in Proc...