Implementing Captcha as Graphical Passwords Based on Hard AI Problems

U. Anitha
Student
Department of Information Technology
Karpaga Vinayaga College Of Engineering And Technology, Kanchipuram Dt. TamilNadu, India

S. Shakila
Student
Department of Information Technology
Karpaga Vinayaga College Of Engineering And Technology, Kanchipuram Dt. TamilNadu, India

V. Kavitha
Assistant Professor
Department of Information Technology
Karpaga Vinayaga College Of Engineering And Technology, Kanchipuram Dt. TamilNadu, India

Abstract

We present captcha as graphical passwords in many security primitives square measure supported laborious mathematical issues. Exploitation laborious AI issues for security is rising as an exciting new paradigm, however has been beneath explored. During this paper, we have a tendency to gift a brand new security primitive supported laborious AI issues, namely, a unique family of graphical watchword systems designed on high of Captcha technology, that we have a tendency to decision Captcha as graphical passwords (CaRP). CaRP is each a Captcha and a graphical watchword theme. CaRP addresses variety of security issues altogether, like on-line guess attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. Notably, a CaRP watchword is found solely probabilistic ally by automatic on-line guess attacks although the watchword is within the search set. CaRP additionally offers a unique approach to deal with the well-known image hotspot drawback in standard graphical watchword systems, like Pass Points, that usually ends up in weak watchword decisions. CaRP isn't a nostrum, however it offers cheap security and usefulness and seems to suit well with some sensible applications for rising on-line security.

Keywords: Online security, AI, Security of data, CARP passwords, Captcha as a graphical passwords, Passpoints, Automatic online guessing attacks, Hard AI problems, Hard mathematical problem, image hotspots problem, Shoulder surfing, Attack, Search set

I. INTRODUCTION

Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. A password authentication system should encourage strong passwords while maintaining memorability. We propose that authentication schemes allow user choice while influencing users toward stronger passwords. We applied this approach to create the first persuasive click-based graphical password system, Persuasive Cued Click-Points (PCCP) and conducted user studies evaluating usability and security. 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. Intuitive countermeasures such as throttling logon attempts do not work well for two reasons:

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

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

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

II. EXISTING SYSTEM

Security primitives based on hard mathematical problems. Using hard AI problems for security is emerging as an exciting new paradigm, but has been underexplored. A FUNDAMENTAL task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. In ccp, users click one point on each of 5 images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake
when entering their latest click-point (at which point they can cancel their attempt and retry from the beginning). It also makes attacks based on hotspot analysis more challenging. Each click results in showing a next-image, in effect leading users down a “path” as they click on their sequence of points. While the predictability problem can be solved by disallowing user choice and assigning passwords to users, this usually leads to usability issues since users cannot easily remember such random passwords. Number of graphical password systems have been developed, Study shows that text-based passwords suffers with both security and usability problems.

A. Limitations of Existing System:
- Using hard AI (Artificial Intelligence) problems for security, initially proposed in [17], is an existing new paradigm.
- Under this paradigm, the most notable primitive invented is Captcha, which distinguishes human users from computers by presenting a challenge.

III. Related works

A large number of graphical password schemes have been proposed. They can be classified into three categories according to the task involved in memorizing and entering passwords: recognition, recall, and cued recall. Each type will be briefly described here. More can be found in a recent review of graphical passwords [1]. A recognition-based scheme requires identifying among decoys the visual objects belonging to a password portfolio. A typical scheme is Passfaces [2] wherein a user selects a portfolio of faces from a database in creating a password. During authentication, a panel of candidate faces is presented for the user to select the face belonging to her portfolio. This process is repeated several rounds, each round with a different panel. A successful login requires correct selection in each round. The set of images in a panel remains the same between logins, but their locations are permuted. Story [20] is similar to Passfaces but the images in the portfolio are ordered, and a user must identify her portfolio images in the correct order. Déjà Vu [21] is also similar but uses a large set of computer generated “random-art” images. Cognitive Authentication [22] requires a user to generate a path through a panel of images as follows: starting from the top-left image, moving down if the image is in her portfolio, or right otherwise. The user identifies among decoys the row or column label that the path ends.

IRCs have also been studied. Asirra was found to be susceptible to machine-learning attacks [24]. IRCs based on binary object classification or identification of one concrete type of objects is likely insecure [25]. Multi-label classification problems are considered much harder than binary classification problems. Captcha can be circumvented through relay attacks whereby Captcha challenges are relayed to human solvers, whose answers are fed back to the targeted application.

IV. Proposed System

We present a 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) on two CaRP schemes that we have implemented among decoys the row or column label that the path ends. 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 PassPoints, 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. We present exemplary CaRPs built on both text Captcha and image-recognition Captcha. 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. To create detailed vector user has to select sequence of images and clicks on each image at click points of his choice. Profile vector is created.
V. ARCHITECTURE

VI. SCENARIO

A. Viewport Selection Module:
In our project, first we brows and select an image for our security process. In that image we put viewport selection. This viewport is movable in overall image. We select image pixels in that viewport only.

B. Fixing Tolerance Level:
Tolerance level used for get coordinated pixels for our selected click points in our image.

C. Selecting Pixels Coordination:
In registration process, we select an image and click anyone pixels in that image. That information is stored in our database for particular user.
D. Encrypting the Data:
In registration process, our all information stored our database in encrypted form. We can use Data Encryption Standard (DES) algorithm for encrypt and decrypt process.

E. Application Maintenance:
Final module of our project as application maintenance. That is, to maintain our application with more and more security. Such as username and image click points.

F. Data Flow Diagram:

![Data Flow Diagram](image)

Fig. 2: Data Flow Diagram

VII. CONCLUSION

We have proposed CaRP, a new security primitive relying on unsolved hard 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. A password of CaRP can be found only probabilistically by
automatic online guessing attacks including brute-force attacks, a desired security property that other graphical password schemes lack. Hotspots in CaRP images can no longer be exploited to mount automatic online guessing attacks, an inherent vulnerability in many graphical password systems. CaRP forces adversaries to resort to significantly less efficient and much more costly human-based attacks. In addition to offering protection from online guessing attacks, CaRP is also resistant to Captcharelay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. CaRP can also help reduce spam emails sent from a Web email service. Our usability study of two CaRP schemes we have implemented is encouraging. For example, more participants considered AnimalGrid and Click Text easier to use than PassPoints and a combination of text password and Captcha. Both AnimalGrid and ClickText had better password memorability than the conventional text passwords. On the other hand, the usability of CaRP can be further improved by using images of different levels of difficulty based on the login history of the user and the machine used to log in. The optimal trade-off between security and usability remains an open question for CaRP, and further studies are needed to refine CaRP for actual deployments.

Like Captcha, CaRP utilizes unsolved AI problems. However, a password is much more valuable to attackers than free email account that Captcha is typically used to protect. Therefore there are more incentives for attackers to hack CaRP than ordinary Captcha. That is, more efforts will be attracted to the following win-win game by CaRP than ordinary Captcha:
If attackers succeed, they contribute to improving AI by providing solutions to open problems such as segmenting 2D texts. Otherwise, our system stays secure, contributing to practical security. As a framework, CaRP does not rely on any specific Captcha scheme. When one Captcha scheme is broken, a new and more secure one may appear and be converted to a CaRP scheme. Overall, 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.

REFERENCES