

A Novel Graphical Password Authentication Scheme

¹L. Lakshmi reddy & ²J. Nagamuneiah

¹M.Tech (CSE), CREC, Tirupati, Email Id: lakshmireddy49@gmail.com

²Associate professor, CREC, Tirupati, Email Id: nagamuni513@gmail.com

ABSTRACT

The most common computer authentication method is to use alphanumeric usernames and passwords. This method has been shown to have significant drawbacks. For example, user tends to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. In this paper, 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). 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.

Key Words— Graphical password; password; hotspots; CaRP; Captcha; dictionary attack; password guessing attack; security primitive

I. INTRODUCTION

The most common computer authentication method is for a user to submit a user name and text password. The vulnerabilities

of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also be easily guessed or broken. According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords. On the other hand, passwords that are hard to guess or break are often hard to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts.

To address the problems with traditional Username password authentication, alternative authentication methods, such as biometrics have been used. However, we will focus on another alternative, using pictures as passwords. Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots. However, this new paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications. Is it possible to create any new security primitive based on hard AI problems? This is a challenging and interesting open problem. In this paper, we introduce a new security primitive based on hard AI problems, namely, a novel family of graphical password systems integrating Captcha technology, which we call CaRP (Captcha as graphical Passwords). CaRP is click-based



graphical passwords, where a sequence of clicks on an image is used to derive a password. Unlike other click-based graphical passwords, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every login attempt. The notion of CaRP is simple but generic. CaRP can have multiple instantiations. In theory, any Captcha scheme relying on multiple-object classification can be converted to a CaRP scheme. CaRP requires solving a Captcha challenge in every login. This impact on usability can be mitigated by adapting the CaRP image's difficulty level based on the login history of the account and the machine used to log in.

Typical application scenarios for CaRP include:

- 1) CaRP can be applied on touch-screen devices whereon typing passwords is cumbersome, esp. 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.

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

2. BACKGROUND

Various graphical password schemes have been proposed as alternatives to text-based passwords. Research has shown that text-based passwords are filled with both usability and security problems that make them less desirable

solutions. Studies revealed that the human brain is better at recognizing and recalling images than text. Graphical passwords are meant to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by images, more secure passwords can be produced and users will not resort to unsafe practices in order to cope.

Graphical passwords may offer better security than text-based passwords because most of the people, in an attempt to memorize text-based passwords, use plain words (rather than the jumble of characters). A dictionary search can hit on a password and allow a hacker to gain entry into a system in seconds. But if a series of selected images is used on successive screen pages, and if there are many images on each page, a hacker must try every possible combination at random.

3. RELATED WORK

Graphical password schemes can be grouped into three general categories: recognition, recall, and cued recall. Recognition is the easiest for human memory whereas pure recall is most difficult since the information must be accessed from memory with no triggers. Cued recall falls between these two as it offers a cue which should establish context and trigger the stored memory.

3.1. Passfaces

Passfaces is a graphical password scheme based primarily on recognizing human faces. During password creation, users select a number of images from a larger set. To log in, users must identify one of their pre-selected images from amongst several decoys. Users must correctly respond to a number of these challenges for each login. Davis et al implemented their own version called Faces and conducted a long-term user study. Results showed that users could accurately remember their images but that user-chosen

passwords were predictable to the point of being insecure.

3.1.2 Story

Davis et al proposed an alternative scheme, Story uses everyday images instead of faces, requires that users select their images in the correct order. Users were encouraged for creating a story as a memory aid. It results in somewhat worse than Faces for memorability, but user choices were much less predictable.

3.1.3 Passpoint



Fig. 1: Graphical Password Authentication using Pass point

Wieden beck et al proposed Pass Points, where passwords could be composed of several points anywhere on an image. They also proposed a “robust discretization” schema, with number of overlapping grids, allowing for login attempts that were closely resembling correct to be accepted and converting the entered password into a cryptographic verification key.

3.1.4 Cued Click Point

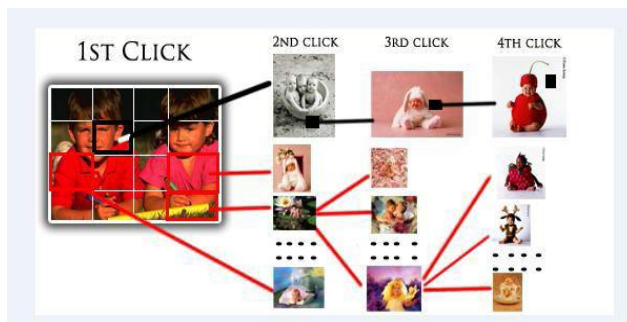


Fig. 2: Graphical Password Authentication using Cued Click Point.

Cued Click Points (CCP) is a proposed alternative to Pass Points. In CCP, users click one point on each image 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. It also makes attacks based on hotspot analysis more challenging.

3.2 RECALL BASED TECHNIQUES

A user is asked to reproduce something that he or she created or selected earlier during the registration stage. Jermyn proposed a technique, called “Draw-a - secret (DAS)” allows the user to draw their unique password . A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. DAS [Draw-A-Secret] allows the user to draw their unique password. A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated.

CAPTCHA

aptcha relies on the gap of capabilities between humans and bots in solving certain hard AI problems. There are two types of visual Captcha: text Captcha and Image-Recognition Captcha (IRC). The former relies on character recognition while the latter relies on recognition of non-character objects. Security of text Captchas has been extensively studied. The following principle has been established: text Captcha should rely on the difficulty of character segmentation, which is computationally expensive and combinatorial hard .

Machine recognition of non-character objects is far less capable than character recognition. IRCs rely on the difficulty of object identification or classification, possibly combined with the difficulty of object segmentation. Asirra relies on binary object classification: a user is asked to identify all the cats from a panel of 12 images of cats and dogs. Security of IRCs has also been studied. Asirra was found to be susceptible to machine-learning attack. IRCs based on binary object classification or identification of one concrete type of objects are likely insecure. 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.

In CaRP, a new image is generated for every login attempt, even for the same user. CaRP uses an alphabet of visual objects (e.g., alphanumeric characters, similar animals) to generate a CaRP image, which is also a Captcha challenge. A major difference between CaRP images and Captcha images is that all the visual objects in the alphabet should appear in a CaRP image to allow a user to input any password but not necessarily in a Captcha image. Many Captcha schemes can be converted to CaRP schemes, as described in the next subsection.

CaRP schemes are clicked-based graphical passwords. According to the memory tasks in memorizing and entering a password, CaRP schemes can be classified into two categories: recognition and a new category, recognition-recall, which requires recognizing an image and using the recognized objects as cues to enter a password. Recognition-recall combines the tasks of both re

cognition and cued-recall, and retains both the recognition-based advantage of being easy for human memory and the cued-recall advantage of a large password space. Exemplary CaRP schemes of each type will be presented later. Like other graphical passwords, we assume that CaRP schemes are used with additional protection such as secure channels between clients and the authentication server through Transport Layer Security (TLS). A CaRP password is a sequence of visual object IDs or clickable-points of visual objects that the user selects.

3.3 RECOGNITION-BASED CARP

For this type of CaRP, a password is a sequence of visual objects in the alphabet. Per view of traditional recognition-based graphical passwords, recognition-based CaRP seems to have access to an infinite number of different visual objects. We present two recognition-based CaRP schemes and a variation next. ClickText

ClickText is a recognition-based CaRP scheme built on top of text Captcha. Its alphabet comprises characters without any visually-confusing characters. For example, Letter “O” and digit “0” may cause confusion in CaRP images, and thus one character should be excluded from the alphabet.



Fig 3: A ClickText image with 33 characters.



Fig 4: Captcha Zoo with horses circled red.



Fig 5: A ClickAnimal image (left) and 6 × 6 grid (right) determined by red turkey's bounding rectangle.

Click Animal

Captcha Zoo is a Captcha scheme which uses 3D models of horse and dog to generate 2D animals with different textures, colors, lightings and poses, and arranges them on a cluttered background. A user clicks all the horses in a challenge image to pass the test. Click Animal is recognition-based CaRP scheme built on top of Captcha Zoo, with an alphabet of similar animals such as dog, horse, pig, etc.

Animal Grid

The number of similar animals is much less than the number of available characters. ClickAnimal has a smaller alphabet, and thus a smaller password space, than ClickText. CaRP should have a sufficiently-large effective password space to resist human guessing attacks.

Recognition Recall CaRP

In recognition-recall CaRP, a password is a sequence of some invariant points of objects. An invariant point of an object (e.g. letter “A”) is a point that has a fixed relative position in different incarnations (e.g., fonts) of the object, and thus can be uniquely identified by humans no matter how the object appears in CaRP images.

Text Points

Characters contain invariant points. A point is said to be an internal point of an object if its distance to the closest boundary of the object exceeds a threshold. A set of internal invariant points of characters is selected to form a set of clickable points for TextPoints. The internality ensures that a clickable point is unlikely occluded by a neighboring character and that its tolerance region unlikely overlaps with any tolerance region of a neighboring character’s clickable points on the image generated by the underlying Captcha engine. In determining clickable points, the

distance between any pair of clickable points in a character must exceed a threshold so that they are perceptually distinguishable and their tolerance regions do not overlap on CaRP images.

TextPoints4CR

For the CaRP schemes presented up to now, the coordinates of user-clicked points are sent directly to the authentication server during authentication. For more complex protocols, say a challenge-response authentication protocol, a response is sent to the authentication server instead. TextPoints can be modified to fit challenge response authentication. This variation is called TextPoints for Challenge-Response or TextPoints4CR.

4. CONCLUSION

We have proposed CaRP, a new security primitive relying on unsolved hard AI problems. CaRP is both a Captcha and 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 Captcha relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. CaRP can also help reduce spamemails 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 ClickText 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 tradeoff 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 a free email account that Captcha is typically used to protect. Therefore there are more incentives for attackers to hack CaRP than 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.

REFERENCES

- [1] 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.
- [2] (2012, Feb.). The Science Behind Passfaces [Online]. Available: <http://www.realuser.com/published/ScienceBehindPassfaces.pdf>
- [3] I. Jermyn, A. Mayer, F. Monroe, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in *Proc. 8th USENIX Security Symp.*, 1999, pp. 1–15.
- [4] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," *Int. J. Netw. Security*, vol. 7, no. 2, pp. 273–292, 2008.
- [5] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *Int. J. HCI*, vol. 63, pp. 102–127, Jul. 2005.
- [6] P. C. van Oorschot and J. Thorpe, "On predictive models and user-drawn graphical passwords," *ACM Trans. Inf. Syst. Security*, vol. 10, no. 4, pp. 1–33, 2008.
- [7] K. Golofit, "Click passwords under investigation," in *Proc. ESORICS*, 2007, pp. 343–358.
- [8] A. E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the passpoints graphical password scheme," in *Proc. Symp. Usable Privacy Security*, 2007, pp. 20–28.
- [9] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot spots in graphical passwords," in *Proc. USENIX Security*, 2007, pp. 103–118.
- [10] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on passpoints-style graphical passwords," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 393–405, Sep. 2010.

[11] P. C. van Oorschot and J. Thorpe, “Exploiting predictability in click-based graphical passwords,” *J. Comput. Security*, vol. 19, no. 4, pp. 669–702, 2011.

[12] T. Wolverton. (2002, Mar. 26). Hackers Attack eBay Accounts [Online]. Available: <http://www.zdnet.co.uk/news/networking/2002/03/26/hackers-attack-ebay-accounts-2107350/>