ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Captcha as Graphical Passwords—a New Security Primitive Based on Hard AI Problems

S.Mounika
M.Tech Student,
Dept of CSE,
KITS for Women's, Kodad, T.S, India.

Mrs.P. Sravanthi
Associate Professor,
Dept of CSE,
KITS for Women's, Kodad, T.S, India.

Abstract:

The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, user tends to pick a 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 conduct a comprehensive survey of the existing graphical password techniques and captcha. Using hard AI problems for security is emerging as an exciting new paradigm, but has been underexplored. In this paper, we present a new security primitive based on hard AI problems, 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 .We discuss the strengths and limitations of each method and point out the future research directions in this area. And also major design and implementation issues are clearly explained. The main advantage of this method is it is difficult to hack.

Keywords:

Graphical password , password, CaRP, Captcha, dictionary attack, password guessing attack, security primitive.

1. 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, usingpictures 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 prob-lem. In this paper, we introduce a new security primitive based on hard AI problems, namely, a novel family of graphical pass-word 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 ebanking 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. RELATED WORK:

A. CAPTCHA:

A CAPTCHA is a program that can generate and grade test that: (A) most humans can pass, but (B) current computer programs cannot pass. Such a program can be used to differentiate humans from computers [5]. There are two types of visual CAPTCHA: text CAPTCHA and Image- Recognition CAPTCHA (IRC).CAPTCHA can be circumvented through relay attacks whereby CAPTCHA challenges are relayed to human solvers [1].

B. GRAPHICAL PASSWORD:

Graphical password schemes have been proposed as apossible alternative to alphanumeric schemes, motivated partially by the fact that humans can remember images easily than text; psychological studies supports such assumption [8]. Images are generally easier to be remembered than text. In addition, if the number of possible images is enough large, the possible password space of a graphical password scheme may exceed that of text-based schemes and thus presumably offer better resistance to dictionary attacks. Because of these (presumed) advantages, there is a increasing interest in graphical password.

In addition to web log-in applications and workstation, graphical passwords have also been applied to mobile devices and ATM machines [6].

3. THE SURVEY:

Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu [1] proposed CaRP scheme. In CaRP i.e. CAPTCHA as gRaphical Passwords, CAPTCHA and graphical password is combined and used as a single entity for authentication. The CaRP schemes are actually click-based graphical passwords with the CAPTCHA technique used in a way that a new image is generated for every login attempt even for the existing user just as CAPTCHAs change everytime. CaRP uses an alphabet set. Instead of actual characters, visual objects i.e. a visual depiction of alphanumeric characters or might be some objects is used for the CaRP image generation which actually turns out to be a CAPTCHA challenge. Noticable difference between normal CAPTCHA and CaRP images is that all objects of an alphabet set for a CaRP scheme are included in every image challenge unlike normal CAPTCHAs where only a part of alphabet set is used.

Many CAPTCHA schemes can be converted to CaRP schemes, as described in the next subsection. On the basis of the memory tasks in memorizing and entering a password, classification of CaRP schemes can be done as follows: recognition based and recognition-recall. The second scheme i.e. recognition – recall CaRP is a new category which works by recognizing an image and using the recognized objects as cues to enter a password. Recognitionrecall combines the tasks of both recognition and cuedrecall. It retains the advantages of both schemes i.e. recognition advantage of being easy for human memory and the cued-recall advantage of a large password space.

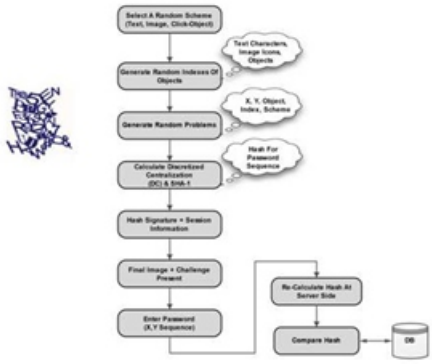

Fig.1 Flowchart of Basic CaRP Authentication of the Proposed Architecture.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Step 1: Enter ID and send it to Authentication server AS. Step 2: AS Stores a salt and hash value H(p, s) for each ID . p is the user password and it is stored. Step 3: Upon receving login request, AS generates a CARP image. It records location of charcters or animals in image and the image is sent to the user. Step 4:

User Clicks the Password. Step 5: Co-ordinates of points are recorded are sent to AS. Step 6: AS maps these Co-ordinates & recovers clickable points of object p, that user clicked. Step 7: Then AS retrieves salt s of account &calculate its hash value with salt using alsorithm like SHA-1. Step 8: IT compares result with hash value stored for the a/c. Step 9: Authentication is successful if and only if the two hash value matched.

• RECOGNITION BASED CaRP

A.CLICKTEXT

Fig. 2. ClickText CaRP Scheme [1]

ClickText is a recognition-based CaRP scheme. It uses text CAPTCHA as its underlying principle. Alphabet set of ClickText comprises alphanumeric characters. A ClickText password is a series of characters in the alphabet, e.g., ρ ="DE@F2SK78", which is similar to a text password. A ClickText image is different from usual CAPTCHA as here all the characters of alphabet set are to be included in theimage.

The underlying CAPTCHA engine generates such CaRP image. When image is generated, each character's location in the image is recorded which would be used in authentication. Characters can be arranged randomly on 2D space in these images which differs from text CAPTCHA challenges where characters are typically ordered from left to right in order for users to type them sequentially.

B.CLICKANIMAL:

Fig. 3. ClickAnimal CaRP Scheme

ClickAnimal is also a recognition-based CaRP scheme. It has an alphabet of similar animals such as dog, horse, pig, etc. The password in this scheme is a sequence of animal names such as ρ = "Cat, Dog, Horse,Turkey,". One or more models are built for every animal. The CAPTCHA generation process wherein 3D models are used to get 2D models by applying different views, colors, lightning effects, textures, and optionally distortions are used for generating the Click Animal image. The resulting 2D animals are then arranged on a cluttered background like grasslands. Some animals may be overlapped by other animals in the image, but their core parts are not overlapped in order for humans to identify each of them. The number of imilar animals is much less than the number of available characters. ClickAnimal has a smaller alphabet, and thus a smaller password space, than ClickText.

C.ANIMALGRID:

Fig. 4. A Click Animal Image (Left) and 6×6 Grid (Right) Determined by Red Turkey's Bounding Rectangle [1]

In order to resist human guessing attacks, a sufficientlylarge effective password space should be present for CaRP schemes. If the ClickAnimal scheme be combined with gridbased graphical passwords, its password space can be increased. The grid can be made depending on the size ofthe selected animal. For authentication process, a ClickAnimal image is displayed first. After an animal is selected, an image of n×n grid appears, with the grid-cell size equaling the bounding rectangle of the selected animal.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Each grid-cell is labeled to help users identify. It has the advantage that a correct animal should be clicked in order for the clicked grid-cell(s) on the follow-up grid to be correct. If a wrong animal is clicked, the follow-up grid is wrong. A click on the correctly labeled grid-cell of the wrong grid would likely produce a wrong grid-cell at the authentication server side when the correct grid is used.

4. DISCUSSION:

• Are CaRP as secured as graphical passwords and text based passwords?

A. The Underlying CAPTCHA Security:

Usually a CAPTCHA challenge might contain about 5 to 8 characters. A CaRP image on the other hand might contain about 30 or more characters. The complexity to break a Click-Text image is about α 30 P(N)/(α10P(N)) = α 20 times the complexity to break a CAPTCHA challenge generated by its underlying CAPTCHA scheme[1].

Thus we can get to the conclusion that the CaRP Click-Text image is much harder to break than its underlying CAPTCHA scheme. As a framework of graphical passwords, CaRP does not rely on any specific CAPTCHA scheme. If one CAPTCHA scheme is broken, a new and more robust CAPTCHA scheme may appear and be used to construct a new CaRP scheme.

B. Online Guessing Attacks:

The trial and error process is executed automatically in automatic online guessing attacks. However, dictionaries can be constructed manually. Such attacks can find a password only probabilistically without considering the number of trials. If a password guess in the trials is the correct one, the trial still has a lower chance of succeeding because a machine might not recognize the objects of CaRP in order to enter the correct password.

This is different than the online guessing attacks on existing deterministic graphical passwords where each trial can determine if the tested password guess is the correct password or not. Also, with targeted passwords in the dictionary, attacking existing graphical passwords is successful for brute-force or dictionary attacks.

C. Shoulder-Surfing Attacks:

If graphical passwords are used in public places there are chances of shoulder-surfing attacks taking place. CaRP is not robust to shoulder-surfing attacks by itself. However, combined with certain dual-view technology, CaRP can thwart shoulder-surfing attacks.• 4.2. Is CaRP vulnerable to relay attacks?There are various ways to carry out relay attacks. Considering CAPTCHA challenges on websites to behacked, one way of attack is to have human surfers solve the challenges to continue surfing the Website. Another way is having relayed to sweatshops where humans are hired to solve CAPTCHA challenges given small payments. The task to perform and the image used in CaRP are very different from those used to solve a CAPTCHA challenge. This noticeable difference makes it hard for a person to mistakenly help test a password guess by attempting to solve a CAPTCHA challenge. Therefore it would be unlikely to get a large number of unwitting people to mount human guessing attacks on CaRP. In addition, human input obtained by performing a CAPTCHA task on a CaRP image is useless for testing a password guess.

5. 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 Captcha relay 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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. 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.

9.ACKNOWLEDGMENTS:

I am S.MOUNIKA and would like to thank the publishers, researchers for making their resources material available. I am greatly thankful to Associate Prof:MRS.P. SRAVANTHI for their guidance. We also thank the college authorities, PG coordinator and Principal for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

6.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. Monrose, 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 passwordsystem," Int. J. HCI, vol. 63, pp. 102–127, Jul. 2005.

[6] P. C. van Oorschot and J. Thorpe, "On predictive models and userdrawngraphical 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 thepasspoints graphical password scheme," in Proc. Symp. Usable PrivacySecurity, 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 clickbased graphical passwords," J. Comput. Security, vol. 19, no. 4, pp. 669–702, 2011.

Author's Details:

Ms.S.Mounika. MTech student, in M.Tech Student, Dept of CSE in KITS for women's,kodad, T.S, India

Mrs.P. Sravanthi working as a Associate at CSE in KITS for women's,kodad, T.S, IndiaJNTUH Hyderabad. He has 2 years of UG/PG Teaching Experience.