© 2016 IJSRSET | Volume 2 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Review Paper on Improved Security Using Captcha as Graphical Password

Priyanka J. Charde, Prof. M. S. Khandare
Department of computer science and technology, Amaravti University, Jagadambha College of Engineering and Technology, Yavatmal, Maharashtra, India

ABSTRACT

Many security primitives are based on hard mathematical problems. 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, 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.

Keywords: Graphical password, password, hotspots, CaRP, Captcha, dictionary attack, password guessing attack, security primitive.

I. INTRODUCTION

A fundamental task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. For example, the problem of integer factorization is fundamental to the RSA public-key cryptosystem and the Rabin encryption. The discrete algorithm problem is fundamental to the ElGamal encryption, the Diffie- Hellman key exchange, the Digital Signature Algorithm, the elliptic curve cryptography and so on. Using hard AI (Artificial Intelligence) problems for security, initially proposed in [12], is an exciting new paradigm. Under this paradigm, the most notable primitive invented is Captcha, which distinguishes human users from computers by presenting a challenge, i.e., a puzzle, beyond the capability of computers but easy for humans. 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. 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 [10]. 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 [9]) and incurs expensive helpdesk costs for account reactivation.
2) It is vulnerable to global password attacks [11] 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 [13] 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. 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.
2) 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. The remaining paper is organized as follows.

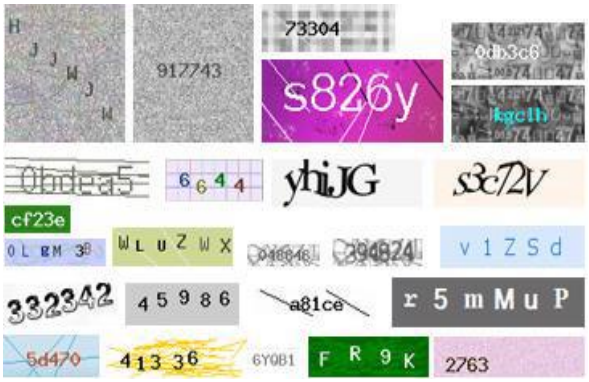

Figure 1. CAPTCHA

II. METHODS AND MATERIAL

1. The Survey and Literature Review

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 every time. 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. Noticeable 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.

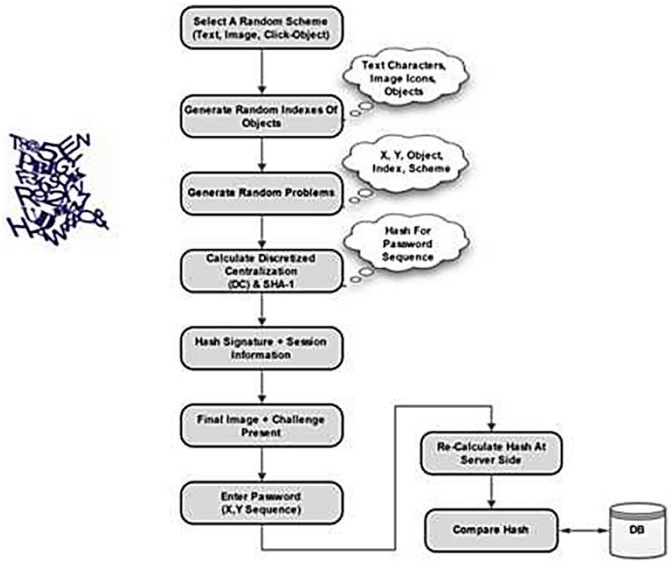

Figure 2. Flow diagram of Captcha

2. Related Work

Captcha

Captcha relies on the gap of capabilities between humans and bots in solving certain hard AI problems. A CAPTCHA is a program that can generate and grade tests 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. Text Captcha should rely on the difficulty of character segmentation, which is computationally expensive and combinational hard.

Graphical Password

Graphical password schemes have been proposed as a possible 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 addition to web log-in applications and workstation, graphical passwords have also been applied to mobile devices and ATM machines [6].

Clicktext

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 the image. 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 [1].

Figure 3. ClickText CaRP Scheme

Clickanimal

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 ClickAnimal 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 similar animals is much less than the number of available characters.

ClickAnimal has a smaller alphabet, and thus a smaller password space, than ClickText [1].

Figure 4. Captcha Zoo with horses circled red.

Graphical password schemes can be grouped into three general techniques:

- recognition based
- pure recall based
- cued recall based

a. Recognition Based Technique

In RBT users have to select pictures, icons or symbols from a pool of images. During the authentication process, the users have to recognize their registration choice from a grid of image such as pass faces, story scheme, picture password and many more.

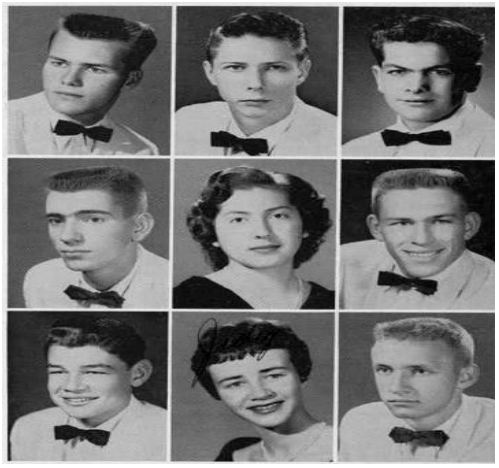

Figure 5. One way Measurement

b. Pure Recall-based Technique

In PRBT, without any clue or hint user generate his password. It follows many algorithms, which include pass doodle, DAS (draw-a-secret) and many more. Recognition inhibits the common use of the Pass doodle. Length and identifiable features of the doodle provides the boundaries of the system. A distinct number of computer differentiable doodles are possible. The doodle here is used as the only means of identification.

c. Cued Recall-based Technique

In CRBT, the image cues the user. For eg. to click a set of option a set of point on an image means hint and reminder help user to reproduce their passwords. It follows many algorithms, which include pass points, CCP(cued click points), PCCP(Persuasive cued click points).

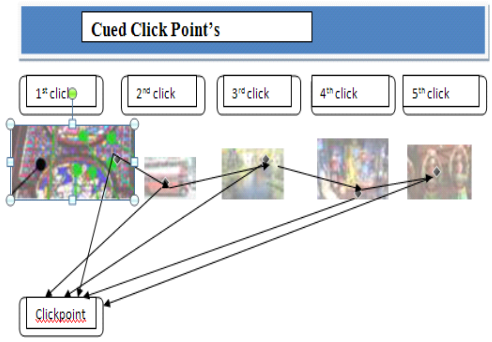

Figure 6. Cued Click Points

3. Security Analysis

A. Security of Underlying Captcha

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 According to [10], the complexity of object segmentation, *C*, is exponentially dependent of the number *M* of objects contained in a challenge, and polynomially dependent of the size *N* of the Captcha alphabet: $C = \alpha M P(N)$, where $\alpha > 1$ is a parameter, and $P()$ is a polynomial function. A Captcha challenge typically contains 6 to 10 characters, whereas a CaRP image typically contains 30 or more characters. The complexity to break a Click-Text image is about $\alpha 30P(N)/(\alpha 10P(N)=\alpha 20$ times the complexity to break a Captcha challenge generated by its underlying Captcha scheme. Therefore ClickText is much harder to break than its underlying Captcha scheme.

B. Automatic online guessing Attack

In automatic online guessing attacks, the trial and error process is executed automatically whereas dictionaries can be constructed manually. If we ignore negligible probabilities, CaRP with underlying CPA-secure Captcha has the following properties: Internal object-points on one CaRP image are *computationally-independent* of internal object-points on another CaRP image. Particularly, clickable points on one image are computationally-independent of clickable points on another image.

C. Human Guessing Attacks

In human guessing attacks, humans are used to enter Passwords in the trial and error process. Humans are much slower than computers in mounting guessing attacks. For 8-character passwords, the theoretical password space is 338 ≈ 240 for ClickText with an alphabet of 33 characters, 108 ≈ 226 for ClickAnimal with an alphabet of 10 animals, and 10 × 467 ≈242 for AnimalGrid with the setting as ClickAnimal plus 6×6 grids. If we assume that 1000 people are employed to work 8 hours per day without any stop in a human guessing attack, and that each person takes 30 seconds to finish one trial. It would take them on average 0.5 · 338 · 30*/ (*3600 · 8 · 1000 · 365*)* ≈ 2007 years to break a ClickText password, 0.5 · 108 · 30*/(*3600 · 8 · 1000*)* ≈ 52 days to break a ClickAnimal password, or 0.5 · 10 · 467 · 30*/(*3600 · 8 · 1000 · 365*)* ≈ 6219 years to break an AnimalGrid password. Human guessing attacks on TextPoints require a much longer time than those on ClickText since TextPoints has a much larger password space.

D. Relay Attacks

Relay attacks may be executed in several ways. Captcha challenges can be relayed to a high-volume Website hacked or controlled by adversaries to have human surfers solve the challenges in order to continue surfing the Website, or relayed to sweatshops where humans are hired to solve Captcha challenges for small payments.

E. Shoulder-Surfing Attacks

Shoulder-surfing attacks are a threat when graphical passwords are entered in a public place such as bank ATM machines. CaRP is not robust to shoulder-surfing attacks by itself. However, combined with the following dual-view technology, CaRP can thwart shoulder-surfing attacks. common implementations of graphical password schemes such as PassPoints use a static input image in the same location of the screen for each login attempt. Although this image can be hidden as the private image by the dual-view technology from being captured by a shoulder surfer, the user-clicked points captured in a successful login are still the valid password for next login attempt. That is, capturing the points alone is sufficient for an effective attack in this case. In general, the higher the correlation of user-clicked points between different login attempts is, the less effective protection he dual-view technology would provide to thwart shoulder surfing attack.

III. RESULTS AND DISCUSSION

Proposed System

Our system is based on Recognition Technique. In this three different group of image is used in that 1.Famous Places 2. Famous People3.Reputed Company Name. Each group contains 25 images. User has to select at least one image from each group during registration phase. During login time user has to click on that images which is selected during registration phase. This system provide protection against shoulder surfing attack, dictionary attack, brute force attack using text password as well as graphical password.

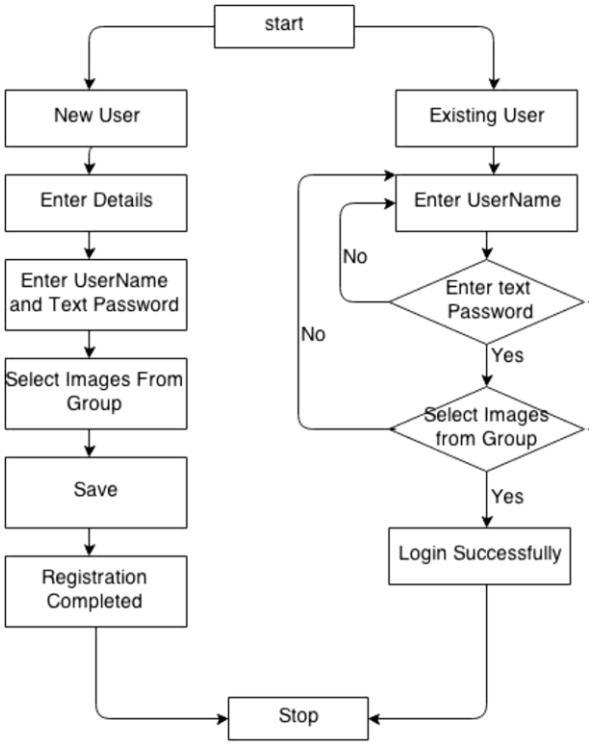

Figure 7. Working Flow of Captcha

IV. CONCLUSION

In this Article, we are implementing Captcha as Graphical Passwords which will be 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. 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. In the implemented module a CaRP image for particular user will get generated. User can sign up by giving his/her username and password. Password is displayed in CaRP image which is combination of password characters and non-password characters.

V. 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 Pass faces 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, "Pass Points: 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] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot spots in graphical passwords," in Proc. USENIX Security, 2007.

[9] 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.

[10] HP Tipping Point DVLabs, Vienna, Austria. (2010). Top Cyber Security Risks Report, SANS Institute and Qualy Research LabsOnline].Available:http://dvlabs.tippingpoint.com/toprisks2010.

[11] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in Proc. ACM CCS, 2002, pp. 161–170.

[12] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in Proc. Eurocrypt, 2003, pp. 294–311.

[13] N. Joshi. (2009, Nov. 29). Koobface Worm Asks for CAPTCHAOnline]. Available : http://blogs.mcafee.com/mcafee-labs/koobface-worm-asksfor- CAPTCHA