ISSN:2348-2079

Volume-5 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

A new countersign in graphical captcha based on hard AI problems

1.Ms.C.Navamani,M.Sc.,M.C.A.,M.Phil.,M.E., Assistant Professor
2. Ms. S.Ruba Final M.C.A.
Department of MCA, Nandha Engineering College,(Autonomous), Erode-52.
navamanimca@gmail.com, rubavinoskpp@gmail.com

Abstract: Many security primitives are based on hard mathematical problems. 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. It is a novel family of graphical password systems built on top of captcha technology. It is a graphical password scheme as well as it addresses a number of security problems such as online guessing attacks, relay attacks, shoulder surfing attacks. A CaRP also offers a novel approach to address the image hotspot problem in popular graphical password systems such as passpoints, that lead to week password choices. CaRP is not a proper solution but it offers security and usability for some practical applications for improving online security.

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

I. INTRODUCTION

A fundamental task in security is to create cryptographic primitives based on hard problems that are computationally difficult. For example, the problem of numeral factorization is fundamental to the RSA public-key cryptosystem. The discrete logarithm problem is fundamental to the ElGamal

Encryption, the Diffie-Hellman key exchange, the Digital Signature Algorithm, the elliptic curve cryptography and so on.

The most notable primitive invented is Captcha, which distinguishes from users to computers by presenting a challenge, i.e., a puzzle Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots. CaRP is click-based graphical passwords, where a series of snaps on an image is used to derive a password.

II. METHODOLOGIES

A 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. 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

One of them is a text CaRP where in 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. Defense against online dictionary attacks is a more subtle problem than it might appear. CaRP also offers protection against relay attacks, an increasing threat to bypass Captcha 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.

III. BACKGROUND AND RELATED WORK

A. Graphical Passwords

- A huge number of graphical password schemes have been suggested. They can be classified into three categories
- According to the task involved in learning and entering passwords: recognition, remembrance, and indicated recall.
- There are two types of visual Captcha: transcript Captcha and Image-Recognition Captcha(IRC). Transcript Captcha should rely on the difficulty of character segmentation, which is computationally expensive and combinatorial hard memorize and enter a password.

B. Captcha

Captcha relies on the gap of expertise between users and bots in solving certain hard AI problems. There are two types of visual Captcha: transcript Captcha and Image-Recognition classification can be converted to a CaRP scheme. Captcha(IRC). Transcript Captcha should rely on the difficulty of character segmentation, which is computationally expensive and combinatorial hard.

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., alphanumerical 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 recog-nized objects as cues to enter a password. Recognition-recall combines the tasks of both recognition 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.

C. Captcha in Authentication

It was introduced in to use both Captcha and password in a user authentication protocol, which we call Captcha-based Password Authentication (CbPA) protocol, to counter real time dictionary attacks.

IV. CAPTCHA AS GRAPHICAL PASSWORDS

A. New Way to Thwart Guessing Attacks

In a guessing attack, a password guess tested in an unsuccessful trial is established wrong and excluded from succeeding trials. Mathematically, let S be the set of password guesses before any trial, ρ be the password to find, T denote a trial whereas Tn denote the n-th trial, and$p(T = \rho)$ be the probability that ρ is tested in trial T. Let En be the set *of password guesses tested in trials up to (including) Tn. The password guess to be tested in n-th trial Tn is from set S\En−1,i.e., the relative complement of En−1 in S. memorize and enter a password.*

B. CaRP: An Overview

In CaRP, a new image is generated for every login challenge,even for the same user. CaRP uses an alphabet of visual objects e.g alphanumerical characters, similar animals) to generate a CaRP image, which is also a Captcha task.

C. Converting Captcha to CaRP

In principle, any visual Captcha scheme depend on recognizing two or more predefined types of objects can be converted to a CaRP. All text Captcha structures and most IRCs meet this requirement.

D. User Authentication With CaRP Schemes

Assume that CaRP schemes are used with additional protection such as secure channels between clients and the authentication server through Transport Layer Security (TLS).

V. RECOGNITION-BASED CaRP**:**

For this type of CaRP, a password is a sequence of visual objects in the alphabet.

A. ClickText

ClickText is a recognition-based CaRP patterns built on top of transcript Captcha. Its alphabet includes 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. A ClickText password is a arrangement of characters in the script, e.g., ρ =“AB#9CD87”, which is related to a text password.

This is different from text Captcha task in which characters are usually ordered from left to right. in order for users to type them successively. a ClickText image with an alphabet of 33 characters. In entering a password, the user snaps on this image the characters in her password, in the same order, for example “A”, B”, “#”, “9”,“C”, “D”, “8”, and then “7” for password ρ = “AB#9CD87”.

B. ClickAnimal

ClickAnimal is a recognition-based CaRP pattern built on top of Captcha Zoo, with an alphabet of alikeanimals such as dog, horse, Character identification is required in locating clickable points on a TextPoints image although the clickable points are known for each character. This is a task outside a bot’s capability.

VI. RECOGNITION-RECALL CaRP:

In recognition-recall CaRP, a password is a series of some invariant points of objects. Each password point has a acceptance range that a click within the tolerance range is acceptable as the password point

A.TextPoints

Characters contain invariant points. which offers a strong cue to memorize and locate its invariant points. A set of internal invariant points of characters is selected to form a set of clickable pointsforTextPoints.

VII. SECURITY ANALYSIS

A. Security of Underlying Captcha

Computational intractability in identifying objects in CaRP images is fundamental to CaRP. surviving analyses on Captcha security were mostly case by case or used an exact process. A Captcha challenge typically contains 6 to 10 characters, whereas a CaRP image usually contains 30 or more characters.

B. Automatic Online Guessing Attacks

In routine online predicting attacks, the trial and error process is performed automatically whereas dictionaries can be made manually.

C. Human Guessing Attacks

In human predicting attacks, users are used to enter passwords in the trial and error process. Humans are much slower than system in rising guessing attacks.

D. Relay Attack

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

E. Shoulder-Surfing Attacks

Shoulder-surfing attacks are a hazard when graphical passwords are entered in a public place such as bank ATM machines. CaRP is not hardy to shoulder-surfing attacks by itself.

F. Other

CaRP is not secure to all possible attacks. CaRP is helpless if a client is compromised such that both the image and user-clicked points can be captured.

VIII. BALANCE OF SECURITY AND USABILITY

Some designs of CaRP offer suitable usability across common device types, e.g. our usability studies used 400 × 400 images, which fit present of smart phones and computers. Expanding alphabet size produces a larger password space,and thus is more protected, but also leads to more complex CaRP images.

Advanced Mechanisms

The CbPA-protocols described in Section II-C need a user to solve a Captcha challenge in addition to entering a password under certain conditions. The scheme described in applies a Captcha challenge when the number of failed login attempts has reached a threshold for an account.

IX. CONCLUSION

We have suggested CaRP, a new security primitive depend on unsolved hard AI problems.A password of CaRP can be found only probabilistically by automatic online guessing attacks including brute-force attacks, a chosen security property that other graphical password arrangements lack.Hotspots in CaRP images can no longer be exploited to support automatic real time predicting attacks.

Overall, our work is one step forward in the paradigm of using hard AI problems for security. Of realistic security and usability and practical improvements, CaRP has good potential

for modifications, which call for useful future work.More importantly, we think CaRP to motivate new discoveries of such AI based security primitives.

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 SecuritySymp.*, 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 userdrawn 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 PrivacySecurity*, 2007, pp. 20–28.

[9] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot potsingraphical 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.

[12] T. Wolverton. (2002, Mar. 26). Hackers AttackeBayAccounts[Online].Available:http://www.et.co.uk/news/networking/2002/03/26/hackers-sattack-ebay-accounts2107350/