Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A New Security Primitive to Improve Security Using AI Techniques

A. Sandhya Rani*, S. L. Sailaja, B. Kishore Kumar Reddy
Assistant Professor, Computer Science and Engineering,
Sri Venkateswara Institute of Technology,
Anantapur, India

***Abstract*— Many security protocols are developed based on hard problems related to mathematics. By using hard AI problems for security is latest as an exciting new hierarchy, but has not been explored. Here, we show a new security constraint which is based on hard AI problems. Some of the hard artificial problems are a novel family of password systems that are graphical built on top of Captcha technology. This is so called as Captcha as graphical passwords, Captcha as graphical passwords.**
Captcha as graphical passwords is combination of a Captcha and a graphical password scheme. Captcha and a graphical password schema address a number of security problems. Some of the security problems are such as guessing attacks done online, relay attacks, and shoulder-surfing attacks(when combined with dual-view technologies). Preferably, a Captcha as graphical passwords password can be found only probabilistically by online guessing attacks done automatically even if the password is in the selected search set. Captcha as graphical passwords also offers a novel approach to represent the well-known image hotspot problem in many popular graphical password systems, such as Pass Points, these often leads to selection of weak password. Captcha as graphical passwords is not a panacea, but it offers trustable usability and security appears to be well coordinated with some practical applications for improving security in online.

Keywords*— Hard AI problems, Graphical password, password , Captcha as graphical passwords, hotspots, Captcha, dictionary attack, password guessing password attack, security constraint.

I. INTRODUCTION

A fundamental thing in security is to create primitives for cryptograph. These primitives are based on hard and tough mathematical problems that are computationally interfacable. For example, the problem of factorization of integers is fundamental to the Rabin encryption and the RSA public-key cryptosystem. The logarithm problem is basic to the ElGamal encryption technique, the Diffie-Hellman key exchange technique, the Digital Signature Algorithm technique, the elliptic curve cryptography technique and so on. Using hard Artificial Intelligence (AI) problems used for security is a new paradigm. Under this paradigm, the most important primitive invented is Captcha, which differentiates human users from computer systems by presenting a challenge in form of a puzzle.

Captcha is a security technique which is now a standard Internet security technique used to protect online emails and other services from being captured by malicious users.

The notion of Captcha as graphical passwords is simple but generic. Captcha as graphical passwords can have multiple instantiations. Theoretically, any Captcha scheme depending on multiple-object classification can be converted to a Captcha as graphical passwords scheme. We present exemplary Captcha as graphical passwords s built on

- text Captcha
- Image-recognition Captcha.

One of them is a text Captcha as graphical passwords. Here, a password is a sequence of characters that is similar like a text password, but entered by clicking the right character sequence based on Captcha as graphical passwords images. Captcha as graphical passwords provides protection against online dictionary attacks upon passwords, this have been acted as a major security threat for long period, for various online services. This threat is widely distributed and considered as most popular cyber security risk. So defence against online dictionary attacks is a more considerable problem than it might appear. Reverse methods such as logon attempts do not work well for two reasons, they are:

1) It causes DOS (denial-of-service) attacks (which were exposed to lock highest bidders out in last minutes of eBay processing) and inhibits expensive helpdesk costs for account re-activation.

2) It is suitable to global password attacks whereby adversaries intend to cut into any account rather than a specific account, and thus check each password user on multiple accounts and enable that the number of trials on each account is less than the threshold to avoid triggering account lockout.

Captcha as graphical passwords also provides protection against relay attacks. Relay attacks are considered as an increasing threat to bypass Captchas protection, wherein Captcha challenges are transferred to humans to solve. One of the examples for relay attack is Koobface. Koobface was a relay attack to overcome Facebook's Captcha in creating new accounts. Captcha as graphical passwords is robust to shoulder-surfing attacks if combined with dual-view technologies.

II. RELATED WORK

The related work is mainly dependent on three various constraints

A. Passwords in graphical manner
B. Captcha as security mechanism
C. Authentication by using Captcha

Passwords in graphical manner:

Previously many number of graphical password schemes have been proposed. But, all of them can be mainly categorized into 3 categories based on entering passwords and memorizing them. They are:

- Recognition based
- Recall based
- Recall cued based

When considering the above three types, recognition is considered as the good and easiest technique for human memory whereas pure recall is considered as the hardest technique. Recognition is typically the weakest while overcoming guessing attacks. Many proposed recognition-based schemes practically have a password space between the ranges of 2^{13} to 2^{16} passwords. Based on the study made on the thesis 6 we reported that a important portion of passwords of Pass-Go and DAS were successfully broken down by using guessing attacks using dictionaries of 2^{31} to 2^{41} entries when compared to the full password space of 2^{58} entries.

Images contain hotspots. Hotspots are nothing but the spots that are selected in creating passwords. Hotspots were derived to mount successful guessing attacks specifically on PassPoints i.e., a important portion of passwords were broken with dictionaries of 2^{26} to 2^{35} entries, as compared to the full space of 2^{43} passwords.

Captcha as security mechanism:

This technique fulfils the gap between the capabilities of users and bots. This technique mainly solves the artificial intelligence problems that are hard. As already seen the captcha is mainly categorized into 2 types:

- Text captcha
- Image recognition captcha

One important principle that is related to captcha is that text captcha should depend on the difficulty of character segmentation, which is hard when combined and expensive when computed

Authentication by using Captcha:

We can use both password and captcha in a user authentication protocol which is introduced in (14). This protocol is called as CbPA(Captcha based password authentication protocol). This protocol is mainly used to counter dictionary attacks that are used online.

Captcha technique was also used with recognition based graphical passwords to show the spyware technique, wherein a text Captcha technique is visualized below each image; a user locates the own pass-images from decoy images, and inputs the characters at specific areas of the Captcha technique below each pass-image as the password during taking permission. These specific areas were selected for each pass-image during creation of password as a part of the password.

In the above schemes, Captcha technique is an independent entity, used together with a graphical or text password. On contrast, a Captcha as graphical passwords is both a Captcha technique and a graphical password scheme, which are intrinsically combined into a single entity.

Other progressive work:

Captcha technique is used to protect sensitive user inputs on an unknown client. This scheme protects the channel used for communication between Web server and user from key loggers and spyware technique, while **Captcha as graphical passwords** is a family of graphical password schemes for user authentication. The paper [35] did not introduce the notion of **Captcha as graphical passwords** or explore its rich properties and the design space of a variety of **Captcha as graphical passwords** instantiations.

III. GRAPHICAL PASSWORDS USING CAPTCHA

Overview:

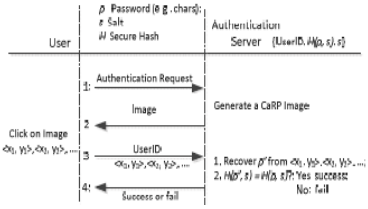

Figure. 1. Flowchart of basic Captcha as graphical passwords authentication

In **Captcha as graphical passwords**, a refreshed image is generated whenever an login attempt is made, even for the same category of user. **Captcha as graphical passwords** uses an *alphabet* of visual objects like alphanumerical characters, to generate a **Captcha as graphical passwords** image, which is also a Captcha challenge.A main difference between **Captcha as graphical passwords** images and Captcha images is that all the objects seen visually in the alphabet should appear in a **Captcha as graphical passwords** image to allow a user to provide any password but not necessarily in a Captcha image. Many Captcha schemes can be converted to **Captcha as graphical passwords** schemes which are discussed in further sections.

Captcha as graphical passwords schemes are clicked based graphical passwords.

Based on the memory techniques in memorizing and entering a password, **Captcha as graphical passwords** schemes can be classified into two categories:

- recognition and a new category
- recognition-recall

Where this requires recognizing an image and using the recognized objects as hints to enter a password. Recognition-recall is combination of the tasks of both recognition and cued-recall, and obtains both the recognition-based advantage of being easy for human memory and the cued-recall advantage of a large password space. Exemplary **Captcha as graphical passwords** schemes of each type will be discussed later.

IV. RECOGNITION-BASED CAPTCHA AS GRAPHICAL PASSWORDS

For this type of **Captcha as graphical passwords** a password is a sequence of objects seen visually in the alphabet. Per view of l recognition based graphical passwords, recognition-based **Captcha as graphical passwords** are uesd to have access to an infinite number of various visual objects. We present two recognition-based **Captcha as graphical passwords** schemes and
a variation next.

- ClickText
- ClickAnimal
- AnimalGrid

Figure. 2. A ClickText image with 33 characters.

Figure. 3. Captcha Zoo with horses circled red.

Figure. 4. A ClickAnimal image

V. RECOGNITION-RECALL CAPTCHA AS GRAPHICAL PASSWORDS

In recognition-recall **Captcha as graphical passwords**, a password is a combination of some invariant points of objects. I*nvariant point* of an object here is letter "A" is a point that has a fixed relative position in different positions like, fonts of the object, and thus can be uniquely identified by humans no matter how the object appears in **Captcha as graphical passwords** images. To input a password, a user should identify various objects in a **Captcha as graphical passwords** image, and then use the founded objects as hints to locate and click the invariant points matching the password.

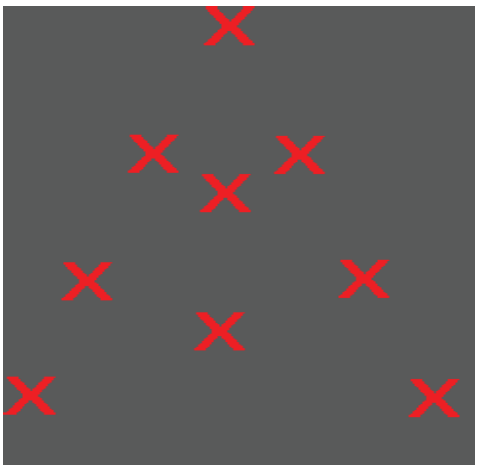

Figure. 5. A Click Animal positions

Each password point has a range of tolerance that a click within the tolerance range is acceptable as the password. Most people have a click differentiation of 3 pixels or less. Text Point, a recognition recall **Captcha as graphical passwords** scheme with an alphabet of characters, is presented next, followed by a variation for challenge response authentication.

VI. CONCLUSIONS

The proposed **Captcha as graphical passwords** is considered as a new security primitive which is dependent on unsolved AI problems and hard AI problems. **Captcha as graphical passwords** is both a graphical password technique and the captcha technique. The notion of **Captcha as graphical passwords** introduces a family of new graphical passwords, which takes a new approach to solve online guessing attacks: a new **Captcha as graphical passwords** image, which is also a Captcha challenge, is used for login attempt every time to make trials of an guessing attack made online, computationally independent of each other. A password of **Captcha as graphical passwords** can be found only *probabilistically* by automatic online guessing attacks which is included with brute-force attacks, a desired security property that other graphical password schemes lack.

Hotspots in **Captcha as graphical passwords** images can no longer be exhibited to mount automatic online guessing attacks which are an inherent vulnerability in many graphical password systems. **Captcha as graphical passwords** forces adversary users
to resort less efficient and more expensive human-based attacks. In addition to offering security from guessing attacks made online, **Captcha as graphical passwords** is also resistant to Captcha relay attacks and if combined with dual view technologies and shoulder-surfing attacks. **Captcha as graphical passwords** can also help reduce emails in spam sent from a Web email service.

Our study of two **Captcha as graphical passwords** schemes we have implemented is encouraging. For example, more participant users considered ClickText and AnimalGrid easier to use when compared with PassPoints and a combination of Captcha and text passwords. Both ClickText and AnimalGrid had better password memorability than the conventional text passwords. Alternatively, the use of **Captcha as graphical passwords** can be then improved by using images of different phases of toughness based on the login history of the machine and the user used to log in.

The minimal tradeoffs between security and usability remains an question for **Captcha as graphical passwords**, and further studies are needed to change **Captcha as graphical passwords** for actual deployments.
Like Captcha, **Captcha as graphical passwords** utilizes unsolved Artificial Intelligence problems.

However, a password is more valuable to attackers than a free email account that Captcha technique is typically used for protection. So, there are more advantages for attackers to hack **Captcha as graphical passwords** than captcha technology. That is, more efforts will be attracted to the following game called win-win by **Captcha as graphical passwords** than ordinary Captcha.

If attackers are successful, they contribute to developing AI by giving solutions to open problems such as segmenting texts in 2D. Otherwise, our system will be secure, contributing to practical security. So, as a framework, **Captcha as graphical passwords** does not depend on any specific Captcha scheme. If one Captcha scheme is broken, a new and more secure one may appear and be converted to a **Captcha as graphical passwords** scheme. Our work is one step forward in the hierarchy of using hard artificial intelligence problems for security. The reasonable security and usability and practical applications, **Captcha as graphical passwords** has good capability for refinements, which is used for useful future work. Importantly, we expect **Captcha as graphical passwords** to motivate new inventions of such artificial intelligence based security primitives.

REFERENCES

[1] (2012, Feb.). *The Science Behind Passfaces* [Online]. Available: http://www.realuser.com/published/ScienceBehindPassfaces.pdf

[2] 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/

[3] HP TippingPoint DVLabs, Vienna, Austria. (2010). *Top Cyber Security Risks Report, SANS Institute and Qualys Research Labs* [Online]. Available: http://dvlabs.tippingpoint.com/toprisks2010

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

[5] P. C. van Oorschot and S. Stubblebine, "On countering online dictionary attacks with login histories and humans-in-the-loop," *ACM Trans. Inf.Syst. Security*, vol. 9, no. 3, pp. 235–258, 2006.

[6] M. Alsaleh, M. Mannan, and P. C. van Oorschot, "Revisiting defenses against large-scale online password guessing attacks," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 1, pp. 128–141, Jan./Feb. 2012.

[7] 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.

[8] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in *Proc. ESORICS*, 2007,pp. 359–374.

[9] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better passwords: Persuasive cued click-points," in *Proc.Brit. HCI Group Annu. Conf. People Comput., Culture, Creativity,Interaction*, vol. 1. 2008, pp. 121–130.

[10] D. Davis, F. Monrose, and M. Reiter, "On user choice in graphical password schemes," in *Proc. USENIX Security*, 2004, pp. 1–11.

