ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

A Survey on CAPTCHA as Pictorial Password Mechanism

Rohit Prakash Vibhandik, Prof. Chhaya Nayak, Nivedita Bhalerao Patil

M. Tech Student, Department of CS, Rajiv Gandhi Proudhyogik Vishwavidyalay, Indore, India

Assistant Professor, Department of CS/ IT, Rajiv Gandhi Proudhyogik Vishwavidyalay, Indore, India

M. Tech Student, Department of CS, Rajiv Gandhi Proudhyogik Vishwavidyalay, Indore, India

ABSTRACT: A lot of security primitives are based on hard mathematical problems. Using hard AI problems for security is evolving as an exciting new paradigm, but has been under-explored. Anew security primitive based on hard AI problems, is a new family of graphical password system based on Captcha technology, which is Captcha as graphical passwords (CaRP). CaRP is togetherly a Captcha and a graphical password system. CaRP addresses a number of security problems altogether, such as online guessing attacks, dependent (relay) attacks and if it is combined with dual-view technologies, also shoulder-surfing attacks. A CaRP password is found only probabilistically by automatic online guessing attacks even though the password is in the search set. CaRP also gives an innovative approach to address the distinguished image hotspot problem in popular graphical password systems, like PassPoints, which often leads to weak password choices. CaRP is not a solution, but it offers practical security and usability and appears well to fit with some practical applications for refining online security.

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

I. INTRODUCTION

A fundamental work in security is to build crypto-graphic primitives based on hard mathematical problems that are computationally unsolvable. For example, integer factorization problem is elementary to the RSA public-key cryptosystem and the Rabin encryption. The discrete logarithm problem is elementary to the ElGamal encryption algorithm, the Diffie-Hellman key exchange algorithm, the Digital Signature Algorithm, the elliptic curve cryptography and a lot many.

Using hard Artificial Intelligence problems for security, initially proposed in [15], is an exciting new prototype. Under this prototype, the most notable primitive developed is Captcha, which distinguishes human users from computers by giving a challenge such as a puzzle. Captcha is a standard Internet security method to protect online email and other services from being mistreated by bots.

However, this new prototype has achieved just a small success as compared to the cryptographic primitives based on hard math problems and their wide applications. To create any new security primitive based on hard AI problems is a challenging and interesting open problem. Solution to this problem is a novel family of graphical password systems integrating Captcha technology, which is called as a CaRP (Captcha as gRaphical Passwords). CaRP is click-based pictorial passwords, It contains a series of clicks on an image which derives a password. This method is distinct from the other click-based pictorial 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. Theorotically any Captcha scheme depending on multiple-object classification can be converted to a CaRP scheme. We present typical CaRPs built on both text Captcha and image-identification Captcha. One of these is a text CaRP where a password is a sequence of characters like a text password and entered by clicking the right character sequence on CaRP images.

CaRP gives protection against online dictionary attacks on passwords which is a major security hazard for many online

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

services. This hazard is common and a top cyber security risk [13]. Defense against online dictionary attacks is a more delicate problem than it appears. Intuitive countermeasures such as throttling log on attempts do not work well for two reasons:

1) Throttling log on attempts causes denial-of-service attacks (which were misused to lock highest bidders out in final minutes of eBay auctions [12]) and causes expensive helpdesk costs for account reactivation.
2) It is susceptible to global password attacks [14] 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 gives protection against relay attacks, an increasing hazard to bypass Captchas protection, whereas Captcha challenges are conveyed to humans to solve. Koobface [6] was a relay attack to bypass Facebook's Captcha in creating new accounts. CaRP is vigorous to shoulder-surfing attacks if it is combined with dual-view technologies.

CaRP requires the solving a Captcha challenge in every login. This impact on usability can be eased by adapting the CaRP image's difficulty level based on the login history of the account and the machine used to log in.

Typical applications for CaRP include:

1. CaRP can be applied on touch-screen devices where typing passwords is bulky specially for secure Internet applications such as e-banks. Many e-banking systems have applied Captchas in user logins [13]. E.g. ICBC is the largest bank in the world, requires to solve a Captcha challenge for every online login.
2. CaRP increases spammer's operating cost and helps reduce spam emails. For an email service provider that uses CaRP, a spam bot cannot log in to an email account even though it is acquainted with the password. Human involvement is necessary to access an account. If CaRP is combined with a policy to control the number of emails sent to new recipients every number of login session, a spam bot can send only a limited emails before asking human assistance for login, leading to reduced outbound spam traffic.

II. RELATED WORK

A. *Graphical Passwords*

A lot of graphical password schemes have been proposed. They are classified into three categories according to the task involved in memorizing and entering passwords: identification, recall, and cued recall. Every type will be briefly described as follows. Evenmore can be found in a recent review of graphical passwords [1].

A recognition-based scheme requires identifying amongst decoys the pctorial objects belonging to a password portfolio. A typical scheme is Passfaces [2] where a user selects a portfolio of faces from a database in creating a password. During the time of authentication, a panel of candidate faces is presented for the user to select the face belonging to his collection. This process is repeated many rounds, every round with a different panel. A successful login requires correct selection in every round. The set of images in a panel remains the same between logins, but their locations are changed. Story [3] is similar to Passfaces but the images in the collection are ordered, and a user must identify his collection images in the accurate order. Cognitive Authentication [12] requires a user to generate a path through a panel of images as follows: starting through the topmost-left image, moving down if the image is in his collection, or right if not. The user identifies amongst decoys the column or row label that the path ends.

This process is repeated every time with a different panel. For a login to be successful requires that the cumulative probability that correct answers were not entered by chance exceeds a threshold within a given number of rounds.

A recall-based scheme requires a user to regenerate the same interaction result without cueing. Draw-A-Secret (DAS) [3] was the first recall-based scheme proposed. A user draws his password on a 2 dimentional grid. The system encodes the series of grid cells along the drawing path as a user-drawn password. Pass-Go [4] improves DAS's usability by encoding the grid intersection points rather than the grid cells. BDAS [3] adds background images to DAS to encourage users to create more complex passwords.

In a cued-recall scheme, an external cue is provided to help memorize and enter a password. PassPoints [5] is a

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

widely studied click-based cued-recall scheme where a user clicks a series of points anywhere on an image in creating a password, and repeated clicks the same series during the time of authentication. Cued Click Points (CCP) [14] is exactly similar to PassPoints but it uses one image for every click, and successive image selected by using deterministic function. Persuasive Cued Click Points (PCCP) [11] extends CCP by requiring a user to select a point inside a randomly positioned viewport when creating a password, resulting in more randomly distributed click-points in a password.

Among the three types, identification is considered the easiest for human memory than pure recall is the hardest [1].Identification is typically the weakest in resisting guessing attacks. Many proposed recognition-based schemes practically have a password space in the range of 2^{13} to 2^{16} passwords [1]. A study [6] reported that a significant portion of passwords of DAS and Pass-Go [4] were successfully broken with guessing attacks using dictionaries of 2^{31} to 2^{41} entries, as compared to the full password space of 2^{58} entries. Images contain hotspots [7], [8], i.e., spots likely selected in creating passwords. Hotspots were broken to mount successful guessing attacks on PassPoints [8]–[11]: a significant portion of passwords were broken with dictionaries of 2^{26} to 2^{35} entries, in comparison with the full space of 2^{43} passwords.

B. *Captcha*

Captcha depends on the gap of capabilities between humans and bots in solving certain hard Artificial Intelligence problems. Mainly two types of visual Captcha: text Captcha and Image-Recognition Captcha (IRC). The former depends on character recognition while the latter relies on recognition of non-character objects. Security of text Captchas has been broadly studied [6]–[10]. The following principle has been established: text Captcha should rely on the difficulty of character segmentation and which is computationally expensive and combinatorially hard [5].

Machine recognition of non-character objects is far less capable than character recognition. IRCs depend on the difficulty of object identification or classification, possibly combined with the difficulty of object segmentation. A user is asked to identify all the cats from a panel of 12 images of cats as well as dogs. Security of IRCs is also been studied and found to be susceptible to machine-learning attacks [4]. IRCs based on binary object classification or identification of one concrete type of objects are likely insecure [15]. Multi-label classification problems are considered much harder than binary classification problems.

Captcha may be circumvented during relay attacks whereby Captcha challenges are depended to human solvers, whose answers are fed back to the targeted application.

C. *Captcha in Authentication*

It was introduced in [14] to use both Captcha and password in a user authentication protocol, which we call Captcha-based Password Authentication (CbPA) protocol, to counter online dictionary attacks. The CbPA-protocol in [14] needs solving of a Captcha challenge after giving a valid pair of user ID and password unless a valid browser cookie is acknowledged. For an unsound pair of user ID and password, the user has a certain probability to solve a Captcha challenge before saying no to the access. A modified CbPA-protocol is proposed in [15] by storing cookies only on user-trusted machines and applying a Captcha challenge only when the number of failed login attempts for the account has exceeded a threshold. It is further improved in [6] by applying a small threshold for failed login attempts from unknown machines but a large threshold for failed attempts from known machines with a previous successful login within a given time frame.

Captcha was also used with recognition-based graphical passwords to address spyware [8, 9], wherein a text Captcha is displayed below each image; a user locates her own pass-images from decoy images, and enters the characters at specific locations of the Captcha below each pass-image as her password during authentication. These specific locations were selected for each pass-image during password creation as a part of the password.

In the above schemes, Captcha is an independent entity, used together with a text or pictorial password. On the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

contrary, a CaRP is both a Captcha and a pictorial password scheme, which are intrinsically combined into a single entity.

D. *Other Related Work*

Captcha is used to protect sensitive user inputs on an untrusted client [15]. This scheme protects the communication channel between user and Web server from keyloggers and spyware, while CaRP is a family of graphical password schemes for user authentication. The paper [15] did not introduce the notion of CaRP or explore its rich properties and the design space of a variety of CaRP instantiations.

III. CAPTCHA AS GRAPHICAL PASSWORDS

A. *A New Way of Guessing Attacks*

A password guess tested in an unsuccessful trial is determined wrong and removed from succeeding trials. The number of unresoluted password guesses goes on decreasing with the number of trials which leads to a better chance of finding the password. Mathematically, Suppose S be the password guesses set before any trial, ρ be the password to find, T denotes a trial where T_n denote the n-th trial, and $p(T = \rho)$ be the probability that ρ is tested in trial T . Let E_n be the set of password guesses tested in trials up to (including) T_n . The password guess to be tested in n-th trial T_n is from set $S\backslash E_{n-1}$, i.e., the relative complement of E_{n-1} in S. If $\rho \in S$, then we have

$$p\,(T = \rho | T_1 \_= \rho\,, \ldots\,, T_{n-1} \_= \rho\,) > p(T = \rho), \qquad (1)$$

And

$$p(T = \rho | T_1 \quad \_= \rho\,, \ldots\,, T_{n-1} \_= \rho\,) \rightarrow 1 \qquad \rightarrow | \quad |$$

$$E_n \rightarrow S \qquad \text{with } n \qquad S\,, \quad (2)$$

where $|S|$ denotes the cardinality of S. From Eq. (2), the password is always get within $|S|$ trials if it is in S; otherwise S I thes exhausted after $|S|$ trials. Every trial determines that if the tested password guess is the actual password or it is not, and the result of the trial is deterministic.

To counter guessing attacks, traditional approaches in designing graphical passwords aim at increasing the effective password space to make passwords harder to guess and thus require more trials. In graphical password scheme, the password can always be searched by a brute force attack. There are two types of guessing attacks: automatic guessing attacks apply an automatic trial and error process but S can be manually constructed and the other one is human guessing attacks apply a manual trial and error process.

CaRP adopts a completely different method to counter automatic guessing attacks. It aims to realize the following equation:

$$p(T = \rho | T_1, \ldots\,, T_{n-1}) = p(T = \rho), \quad \forall n \qquad (3)$$

in an automatic guessing attack. Eq. (3) means that each trial is computationally independent of other trials. Specifically, independent of the trials executed previously, the chance of searching the password in the current trial always remains the same. That is, a password in S can be searched only *probabilistically* by automatic guessing (including brute-force technique) attacks, in contrast to existing graphical password system where a password can be found within a fixed number of trials.

If a fresh image is used for every trial, and images of different trials are independent of each other, then Eq. (3) holds. The independent images amongst different login attempts should contain unique information so that the authentication server can verify applicants. Examining the ecosystem of user authentication, we notice that human users enter passwords during authentication, while the trial and error process in guessing attacks is performed automatically. The capability gap between humans and machines can be misused to generate images so that they are *computationally-independent* yet retain invariants that only humans can iden-tify, and thus use as passwords. The

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

invariants amongst the images should be intractable to machines to automate guessing attacks. This requirement is identicle to an ideal Captcha [14], which leads to creation of CaRP.

B. *CaRP: An Overview*

In CaRP, a new image is generated for every login attempt, eventhough the user is same. CaRP uses an *alphabet* of graphical objects (e.g., alphanumerical characters, similar animals) to generate a CaRP image, which is also a Captcha challenge. A difference between CaRP images and Captcha images is that all the graphical 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.

CaRP systems are clicked-based graphical passwords. According to the memory tasks in memorizing and entering a password, CaRP systems can be classified into two categories: recognition and recognition-recall, which demands recognizing an image and using the recognized objects as cue 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. *Converting Captcha to CaRP*

Any graphical Captcha system depending on recognition of two or more predefined types of objects can be converted to a CaRP. All text Captcha systems and most of the IRCs meet this requirement. Those IRCs that depend on recognition of a single predefined type of objects can also be converted to CaRPs in general by adding more types of objects. Practically, conversion of a specific Captcha system to a CaRP system requires a case by case study, so as to acheive both security and usability.

D. *User Authentication With CaRP Schemes*

Similar to the other graphical passwords, assume that CaRP schemes are used with additional protection like secure channels between clients and the authentication server through Transport Layer Security (TLS). A typical way to apply CaRP scheme in user authentication is as given below. The authentication server *AS* stores a salt *s* and a hash value $H(\rho, s)$ for every user ID, where ρ is the password of the account and which is not stored. A CaRP password is a sequence of visual object IDs or clickable-points of visual objects that the user selects. On reception of a login request, *AS* produces a CaRP image, records the locations of the objects in the image, and sends the image to the user to click her password. The coordinates of the clicked points are stored for the future reference and sent to *AS* along with the user ID.

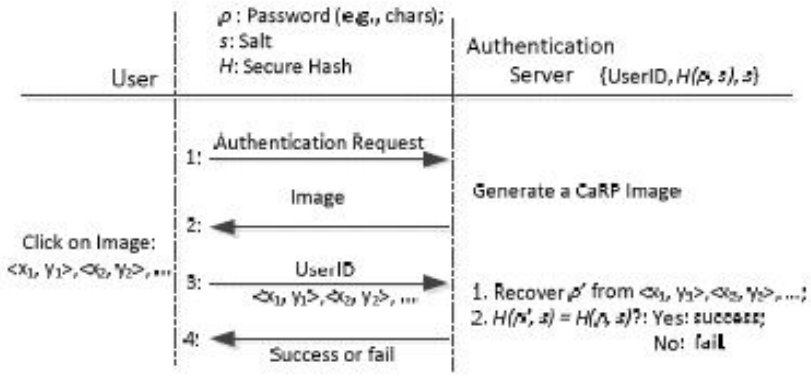

Fig.1. Flowchart of basic CaRP authentication.

AS plots the received coordinates onto the CaRP image, and recovers a sequence of graphical object IDs or clickable points of graphical objects, ρ^-, that the user clicked on the image. Then *AS* retrieves salt *s* of the account, calculates the hash value of ρ^- with the salt, and does the comparison of the result with the hash value stored for the account. Authentication is successful only if the two hash values match. The process is called as the basic CaRP authentication and shown in Fig. 1.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

IV. ADVANTAGES, DISADVANTAGES AND APPLICATIONS OF CAPTCHA AS A GRAPHICAL PASSWORD

ADVANTAGES:

1. Captcha distinguishes in between human and a machine.
2. Captcha is used to make online polls more legitimate.
3. Captcha reduces spam and viruses.
4. Captcha makes online shopping safer.
5. Captcha diminishes abuse of free emailaccount services .

DISADVANTAGES:

1. Sometimes Captchas are very difficult to read.
2. Captchas are not compatible with the user with disabilities.
3. Use of Captcha faces technical difficulties with certain internet browser.
4. Captcha may enhance artificial intelligence greately.

APPLICATIONS:

1. Captcha is mostly used for preventing comment spam
2. Captcha is also helpful in online polling and surveys.
3. Captcha is also known as good spam blocker against the spammers who search the web for email address. One can ask the visitor to solve the complex Captcha to get the email address. It is used as spam blocker also it can be used to protect email address from spam scrapers.
4. Captcha is used to prevent all kinds of bots
5. Captcha is used as free anti-spam.

V. CONCLUSION

CaRP, a new security primitive depending on unsolved hard Artificial Intelligence problems. CaRP is a Captcha and a graphical password systeme too. The idea of CaRP introduces a novel family of graphical passwords, which adopts a novel approach to contradict online guessing attacks: a new CaRP image, which is 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 searched only probabilistically by automatic online guessing attacks including brute-force attacks, a favourable security property that other graphical password schemes not have. Hotspots in CaRP images cannot be misused to mount automatic online guessing attacks. Overall, our work is one step forward in the paradigm of using hard Artificial Intelligence problems for security. Because of Reasonable security and usability and practical applications, CaRP is feasible for refinements which can be for useful future work. More importantly, In future, CaRP to inspire new inventions of such AI based security primitives.

ACKNOWLEDGEMENT

At the time of making a survey on this area many people were helped me. I specially thankful to Prof. Chhaya Nayak, Head of the Dept (CS/IT), B. M. college of Technology & for valuable guidance on this area. Last but not the least we also thank to our Faculty members, staff and friends for being instrumental towards the completion of this paper.

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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

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. ZHU et al.: New Security Primitive Based On Hard Ai Problems
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, 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, 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/
13. HP TippingPoint DVLabs, Vienna, Austria. (2010). Top Cyber Security Risks Report, SANS Institute and Qualys Research Labs [Online]. Available: http://dvlabs.tippingpoint.com/toprisks2010
14. B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in Proc. ACM CCS, 2002, pp. 161–170.
15. 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.