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

Improving Online Security using graphical password systems Built on Captcha Technology

P.Rajya Lakshmi
P.G. Scholar (M. Tech),
Department of CSE,
Modugula Kalavathamma Institute of Technology for Woman,
New Boyanapally, Rajampet.

D.L.Sailaja
Associate Professor
Department of CSE,
Modugula Kalavathamma Institute of Technology for Woman,
New Boyanapally, Rajampet.

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 PassPoints, 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.

Index Terms—Graphical password, password, hotspots, CaRP, Captcha, dictionary attack, password guessing attack, security primitive

I.INTRODUCTION

Security awareness is an important factor in an information security program. While organizations and institutes expand their use of advanced security technology and continuously train their security professionals, fraction of it is used to increase the security awareness among the normal users. As a result, today, organized cyber criminals are trying hard towards research and development of advanced hacking methods that can be used to steal money and secured information from the general public. Password authentication is one of the most common building blocks in implementing access control. Each user has a relatively short sequence of characters commonly referred to as a password. To gain access, providing right password is essential. Common attack for breaking password authenticated systems is dictionary attack [2]. Graphical password is an option for alphanumeric password as text password is slightly hard to remember text password. When any application is provided with user friendly authentication it becomes easy to break and use that application. Cloud security can also be given by alphanumeric password but thing matter is that use of alphanumeric is not that much of secure and easy to remember. Any individual examining the password can memorize it which may lead to its misuse.

Graphical password schemes are more reliable and more resilient to dictionary attacks than textual passwords, but more vulnerable to shoulder surfing attacks [3]. CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) is a program that generates and grades tests that are human solvable, but current computer programs do not have the ability to solve them. The robustness of CAPTCHA is found in its strength in resisting automatic adversarial attacks, and it has many applications for practical security, including free email services, online polls, search engine bots, preventing dictionary attacks, worms and spam [4]. CaRP is a combination of both a CAPTCHA and a graphical password scheme. CaRP overcome a number of security issues, such as relay attacks, online guessing attacks, and,

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

if combined with CAPTCHA and graphical password, shoulder-surfing attacks. CaRP is click-based graphical passwords, where order of clicks on an image is used to get a new password. Unlike other click-based graphical passwords, images used in CaRP are used to generate CAPTCHA challenges, and for every login attempt a new CaRP image is generated whether the existing user tries authenticating or a new user. In this paper we conduct a comprehensive survey of existing CaRP techniques namely ClickText, ClickAnimal and AnimalGrid. We point out research direction in this area. We also try to answer our CaRP as secured as graphical passwords and text based passwords. Survey will be useful for information security researchers and practitioners who are interested in finding an alternative to graphical authentication methods.

II. RELATED WORK

A. CAPTCHA

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 ImageRecognition CAPTCHA (IRC).CAPTCHA can be circumvented through relay attacks whereby CAPTCHA challenges are relayed to human solvers [1].

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

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] requires solving a Captcha challenge after inputting a valid pair of user ID and password unless a valid browser cookie is received. For an invalid pair of user ID and password, the user has a certain probability to solve a Captcha challenge before being denied access. An improved 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 [16] 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 [40], [41], 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. Intheaboveschemes,Captchaisanindependententity,used together with a text or graphical password. On the contrary, a CaRP is both a Captcha and a graphical password scheme, which are intrinsically combined into a single entity.

III. RECOGNITION-BASED CaRP

For this type of CaRP, a password is a sequence of visual objects in the alphabet. Per view of traditional recognition based graphical passwords, recognition-based CaRP seems to have access to an infinite number of different visual objects. We present two recognition-based CaRP schemes and a variation next.

A. ClickText: ClickText is a recognition-based CaRP scheme built on top of text Captcha. Its alphabet comprises characters without any visually-confusing characters. For example, Letter “O” and digit “0”

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

may cause confusion in CaRP images, and thus one character should be excluded from the alphabet. A ClickText password is a sequence of characters in the alphabet, e.g., ρ ="AB#9CD87", which is similar to a text password. A ClickText image is generated by the underlying Captcha engine as if a Captcha image were generated except that all the alphabet characters should appear in the image. During generation, each character's location is tracked to produce ground truth for the location of the character in the generated image. The authentication server relies on the ground truth to identify the characters corresponding to userclicked points.

B. ClickAnimal

Captcha Zoo [32] is a Captcha scheme which uses 3D models of horse and dog to generate 2D animals with different textures, colors, lightings and poses, and arranges them on a cluttered background. A user clicks all the horses in a challenge image to pass the test. Fig. 3 shows a sample challenge wherein all the horses are circled red. ClickAnimal is a recognition-based CaRP scheme built on top of Captcha Zoo [32], with an alphabet of similar animals such as dog, horse, pig, etc. Its password is a sequence of animal names such as ρ = "Turkey, Cat, Horse, Dog" For each animal, one or more 3D models are built. The Captcha generation process is applied to generate ClickAnimal images: 3D models are used to generate 2D animals by applying different views, textures, colors, lightning effects, and optionally distortions. The resulting 2D animals are then arranged on a cluttered background such as grassland. Some animals may be occluded by other animals in the image, but their core parts are not occluded in order for humans to identify each of them. Fig. 4 shows a ClickAnimal image with an alphabet of 10 animals.

C. Animal Grid

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. CaRP should have a sufficiently-large effective password space to resist human guessing attacks. AnimalGrid's password space can be increased by combining it with a grid-based graphical password, with the grid depending on the size of the selected animal. DAS [3] is a candidate but requires drawing on the grid. To be consistent with ClickAnimal, we change from drawing to clicking: Click-A-Secret (CAS) wherein a user clicks the grid cells in her password. AnimalGrid is a combination of ClickAnimal and CAS. The number of grid-cells in a grid should be much larger than the alphabet size. Unlike DAS, grids in our CAS are object-dependent, as we will see next. 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 gridcell at the authentication server side when the correct grid is used.

Fig. 2. A ClickText image with 33 characters.

Fig. 3. Captcha Zoo with horses circled red.

Fig.1. A Click Animal image (left) and 6 × 6 grid (right) determined by red turkey's bounding rectangle.

IV. RECOGNITION-RECALL CaRP

In recognition-recall CaRP, a password is a sequence of some invariant points of objects. An invariant point of an object (e.g. letter "A") is a point that has a fixed relative position in different incarnations (e.g., fonts) of the object, and thus can be uniquely identified by humans no matter how the object appears in CaRP images. To enter a password, a user must identify the objects in a CaRP image, and then use the identified objects as cues to locate and click the invariant points matching her

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

password. Each password point has a tolerance range that a click within the tolerance range is acceptable as the password point. Most people have a click variation of 3 pixels or less [18]. TextPoint, a recognition recall CaRP scheme with an alphabet of characters, is presented next, followed by a variation for challenge response authentication.

A. TextPoints

Characters contain invariant points. Fig. 5 shows some invariant points of letter "A", which offers a strong cue to memorize and locate its invariant points. A point is said to be an internal point of an object if its distance to the closest boundary of the object exceeds a threshold. A set of internal invariant points of characters is selected to form a set of clickable points for TextPoints. The internality ensures that a clickable point is unlikely occluded by a neighboring character and that its tolerance region unlikely overlaps with any tolerance region of a neighboring character's clickable points on the image generated by the underlying Captcha engine. In determining clickable points, the distance between any pair of clickable points in a character must exceed a threshold so that they are perceptually distinguishable and their tolerance regions do not overlap on CaRP images.

Image Generation: TextPoints images look identical to ClickText images and are generated in the same way except that the locations of all the clickable points are checked to ensure that none of them is occluded or its tolerance region overlaps another clickable point's. We simply generate another image if the check fails. As such failures occur rarely due to the fact that clickable points are all internal points, the restriction due to the check has a negligible impact on the security of generated images.

Authentication: When creating a password, all clickable points are marked on corresponding characters in a CaRP image for a user to select. During authentication, the user first identifies her chosen characters, and clicks the password points on the right characters. The authentication server maps each user-clicked point on the image to find the closest clickable point. If their distance exceeds a tolerable range, login fails. Otherwise a sequence of clickable points is recovered, and its hash value is computed to compare with the stored value.

Fig.2. some invariant points (red crosses) of "A".

Clickable points in TextPoints are salient points of their characters and thus help remember a password, but cannot be exploited by bots since they are both dynamic (as compared to static points in traditional graphical password schemes) and contextual.

Dynamic: locations of clickable points and their contexts (i.e., characters) vary from one image to another. The clickable points in one image are computationally independent of the clickable points in another image, as we will see in Section VI-B. □ Contextual: Whether a similarly structured point is a clickable point or not depends on its context. It is only if within the right context, i.e., at the right location of a right character.

B. TextPoints4CR

For the CaRP schemes presented up to now, the coordinates of user-clicked points are sent directly to the authentication server during authentication. For more complex protocols, say a challenge-response authentication protocol, a response is sent to the authentication server instead. TextPoints can be modified to fit challenge-response authentication. This variation is called TextPoints for Challenge-Response or TextPoints4CR. Unlike TextPoints wherein the authentication server stores a salt and a password hash value for each account, the server in TextPoints4CR stores the password for each account. Another difference is that each character appears only once in a TextPoints4CR image but may appear multiple times in a TextPoints image. This is because both server and client

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

in TextPoints4CR should generate the same sequence of discretized grid-cells independently. That requires a unique way to generate the sequence from the shared secret, i.e., password. Repeated characters would lead to several possible sequences for the same password. This unique sequence is used as if the shared secret in a conventional challenge response authentication protocol. Image Generation To generate a TextPoints4CR image, the same procedure to generate a TextPoints image is applied.

Then the following procedure is applied to make every clickable point at least τ distance from the edges of the grid-cell it lies in. All the clickable points, denoted as set _, are located on the image. For every point in _, we calculate its distance along x-axis or y-axis to the center of the grid-cell it lies in. A point is said to be an internal point if the distance is less than 0.5μ−τ along both directions; otherwise a boundary point. Authentication In entering a password, a user-clicked point is replaced by the grid-cell it lies in. If click errors are within τ , each user-clicked point falls into the same grid-cell as the original password point. Therefore the sequence of grid-cells generated from user-clicked points is identical to the one that the authentication server generates from the stored password of the account. This sequence is used as if the shared secret between the two parties in a challenge response authentication protocol.

V. DISCUSSION

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 α30 P(N)/(α10P(N)) = α20 times the complexity to break a CAPTCHA challenge generated by its underlying CAPTCHA scheme[1].

Thus we can get to the conclusion that the CaRPClickText 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 be hacked, 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.

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

VI. RESULTS:

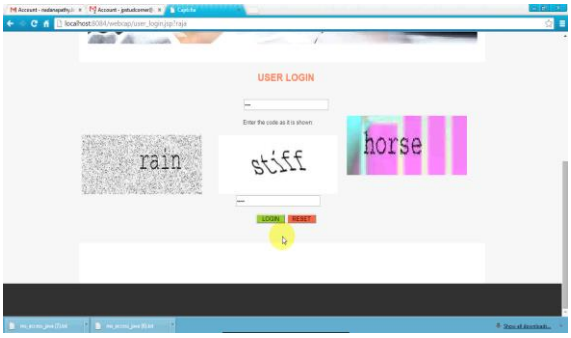

Figure 3.

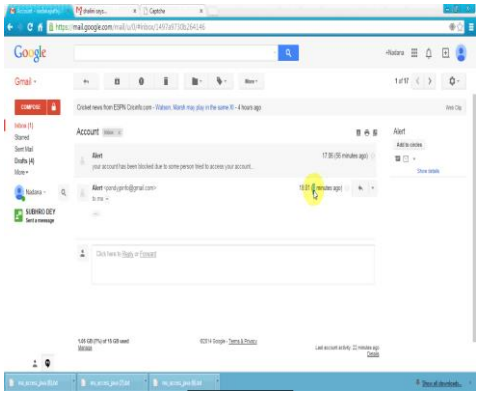

Figure4.

VII 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-forceattacks, 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. 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 improvedby 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.

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 BehindPassfaces [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 password system,” Int. J. HCI, vol. 63, pp. 102–127, Jul. 2005. ZHU et al.: NEW SECURITY PRIMITIVE BASED ON HARD AI PROBLEMS 903

[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.

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

[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, 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 Attack eBay Accounts [Online]. Available: http://www.zdnet.co.uk/news/networking/2002/03/26/hackers-attack-ebay-accounts-2107350