ISSN :2455-0108 Impact Factor : 2015-3.462
IJO–Science
INTERNATIONAL JOURNAL ONLINE OF SCIENCE
Volume II Issue IV July 2016

A REVIEW - CAPTCHA AS GRAPHICAL PASSWORDS—A NEW SECURITY PRIMITIVE BASED ON HARD AI PROBLEMS

PANKAJ

NET (COMPUTER SCIENCE & APPLICATIONS)

B.TECH. (IT)

MCA

MBA (IT & MARKETING)

MAHARSHI DAYANAND UNIVERSITY, ROHTAK

HARYANA

INDIA

ABSTRACT

Most of the safety primeval square measure supported mathematical issues. This analysis goals to check existing parole and to style a brand new improved graphical parole pattern. Captcha as a graphical parole. during this paper, we tend to discuss a brand new security primeval supported exhausting computer science issues, a innovative of graphical parole systems created on dominant of Captcha technology, what we are saying Captcha as graphical passwords (CaRP). CaRP is each a Captcha and a graphical parole pattern. With the mix of CAPTCHA and graphical parole addresses a like on-line estimation attacks, relay attacks, combination of with dual-view technology, and shoulder-surfing attacks. If the parole is in search nominative then CaRP parole are often found solely risk by automatic on-line estimation attack.

Keywords

Graphical Password, Password guessing attack, Shoulder-surfing attacks, Security Primitive, Authentication, Hotspots, Captcha.

1. INTRODUCTION

Now a days, User authentication may be a major drawback in authentication system. And for security, objective of authentication is depends on positive identification. Graphical passwords square measure another to classical text passwords, whereby a user should keep in mind a picture in place of a word. There square measure differing kinds of graphical passwords; among the a lot of common methodes is click-based graphical passwords ,

ISSN :2455-0108 Impact Factor : 2015-3.462
IJO–Science
INTERNATIONAL JOURNAL ONLINE OF SCIENCE
Volume II Issue IV July 2016

which require users to click on a sequence of points on one or multiple background pictures. during this paper we tend to contemplate advance the speculation and apply of graphical passwords. we tend to style 2 graphical positive identification pattern that we tend to bear in mind to be additional secure than matter passwords. mistreatment arduous AI issues for security, A captcha may be a program that may generate and grade tests that:

(A) Most humans will pass

(B) Current pc programs can't pass.

Such a program may be wont to perceive humans from computers and has several applications for sensible security, as well as – on-line Polls. 1999,slashdot.com free an internet poll asking that was the most effective grad school in engineering (a dangerous question to ask round the web!). As is that the case with most on-line polls, informatics addresses of voters were recorded so as to forestall single users from balloting quite once. However, students at Carnegie moneyman found some way to stuff the ballots by mistreatment programs that voted for CMU thousands of times. CMU's score started growing chop-chop. subsequent day, students at MIT wrote their own balloting program and also the poll became a contest between balloting "bots". MIT finished with twenty one,156 votes, Carnegie moneyman with twenty one,032 and each different faculty with but one,000. will the results of any on-line poll be trusted? Not unless the poll needs that solely humans will vote.

– Free Email Services. Most of the businesses (Yahoo!, Microsoft, etc.) offer free email services, that bear from a selected style of attack: "bots" that check in for thousands of email accounts each minute. This position may be increased by demanding users to prove they're human before they will get a free email account. Yahoo!, for instance, uses a captcha of our style to impede bots from registering for accounts. Worms and Spam. Captcha positive identification additionally supply a reputable answer against email worms Associate in Nursingd spam: explicit settle for an email if recognize there's a person's behind the opposite pc.

CaRP provides security against on-line attacks on passwords, that are for long-standing a significant security threat for many on-line services .Defense across on-line lexicon attacks may be a a lot of slight drawback than it would emerge. It causes denial-of-service Associate in Nursing attack verify to clean up a network, produce it inaccessible to its meant users. for instance DoS attack deprives legitimate users the service or resource they expected.

Two general methodologies of DoS attacks

1. Flooding Service (Which occur once the system receives several traffic for the server to buffer, creating them to hamper and ultimately stop.)

2. Blinking Service

CaRP offer protection from relay attacks, Associate in Nursing increasing threat to bypass Captchas protection, whereby Captcha challenges square measure relayed to humans to unravel. CaRP wants solve a Captcha protest in every login Typical theme for Captcha a Graphical include:

CaRP may be implemented on bit screen devices wherever on typewriting passwords is for secure net applications like e-banking, on-line trancations, several e-banking systems, Secure sites have applied Captchas in user logins.

ISSN :2455-0108 Impact Factor : 2015-3.462
IJO–Science
INTERNATIONAL JOURNAL ONLINE OF SCIENCE
Volume II Issue IV July 2016

2. LITERATURE SURVEY

Bin B. Zhu et. al [1] "Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems" during this paper projected CaRP, a replacement security primitive wishing on unresolved onerous AI issues. CaRP is each a Captcha and a graphical positive identification theme. The notion of CaRP introduces a replacement family of graphical passwords, that adopts a replacement approach to counter on-line guesswork attacks: a replacement CaRP image, that is additionally a Captcha challenge, is employed for each login conceive to create trials of a web guesswork attack computationally freelance of every different. A positive identification of CaRP will be found solely probabilistically by automatic on-line guesswork attacks as well as brute-force attacks, a desired security property that different graphical positive identification schemes lack. Hotspots in CaRP pictures will now not be exploited to mount automatic on-line guesswork attacks, associate degree inherent vulnerability in several graphical positive identification systems. CaRP forces adversaries to resort to considerably less economical and far additional expensive human-based attacks. additionally to protectively from on-line guesswork attacks, CaRP is additionally proof against Captcha relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. CaRP may facilitate cut back spam emails sent from an internet email service. Overall, our work is one breakthrough within the paradigm of exploitation onerous AI issues for security. Of cheap security and usefulness and sensible applications, CaRP has sensible potential for refinements, that entail helpful future work. additional significantly, we have a tendency to expect CaRP to inspire new inventions of such AI primarily based security primitives.

Robert Biddle, Sonia Chiasson, P.C. van Oorschot et. al. [2]. "Graphical Passwords: Learning from the First Twelve Years"
In this paper presents Our tour of graphical arcanum analysis reveals an expensive palette of ideas, however few schemes that deliver on the first promise of addressing the illustrious issues with text pass- words. Indeed, review of the primary era of graphical arcanum schemes indicates that several of constant issues still re-surface. For graphical passwords to advance as a heavy authentication different, we have a tendency to believe analysis should be conducted and given in an exceedingly manner permitting systematic examination and comparison of every scheme's main characteristics, showing however every meets the usability and security necessities of specifc target environments the most purpose of authentication schemes is to permit system access solely by legitimate users. To completely assess the safety of a graphical arcanum proposal, and to facilitate comparison with alternatives, all customary threats and illustrious attacks ought to be analyzed, with convincing arguments on however the theme precludes (or falls to) them. Moreover, such security analysis should be in the middle of concrete experimental studies and value analysis.

Hai Tao and Carlisle Adams et. al. [3]. "Pass-Go: A Proposal to Improve the Usability of Graphical Passwords" In this Paper have given a replacement graphical parole theme and shown that it keeps most of the benefits of the DAS theme and offers stronger security and higher usability. Our contributions conjointly embody the following: a replacement categorization of graphical password themes; the introduction of reference aids; associate economical and human clear cryptography scheme; identification of the requirement and an answer for keyboard input

ISSN :2455-0108 Impact Factor : 2015-3.462
IJO–Science
INTERNATIONAL JOURNAL ONLINE OF SCIENCE
Volume II Issue IV July 2016

support; many solutions for the shoulder aquatics problem; a dynamic password checking method; and 3 variations on the essential scheme. we tend to conducted a casual user study and provided careful statistics concerning the characteristics of user-chosen passwords. the most necessary among them is that users tend to decide on very long passwords in our theme, resulting in an especially massive password area.

Robert G. Rittenhous, Junaid Ahsenali Chaudry and Malrey Lee et. al. [4]. "Security in Graphical Authentication " during this paper projected, Graphical user authentication guarantees raised security by permitting additional complicated passwords to be simply remembered by users. additionally, graphical passwords will be created immune to shoulder water sport and even spybots and similar compromises of user systems.Susan Wiedenbecka, Jim Watersa, Jean-Camille Birgetb,Alex Brodskiyc, Nasir Memon et. al. [5]. ”PassPoints: style and longitudinal analysis of a graphical arcanum system”, during this paper propoed on, the empirical testing of PassPoints indicates strengths and weaknesses. Graphical arcanum users were able to simply and quickly produce a sound arcanum, however they'd additional problem learning their passwords than alphanumerical users, taking additional trials and longer to complete the apply. Graphical users’ retention of their arcanum over the course of six weeks was the same as character set users, however the graphical users continued to require longer to input their passwords than character set users. Graphical users had similar perceptions to alphanumerical users in terms of ease and speed of input and pleasantness of their arcanum system.

Haichang Gao, Xiyang Liu, Sidong Wang et. al. [6]. A new graphical password scheme against spyware by using CAPTCHA" In this paper, we've got presented a replacement approach to guard user’s word against spyware attack. Our main contribution is that we tend to introduce CAPTCHA into the realm of graphical passwords. From the safety viewpoint, this exploration is predicted to advance the event of graphical passwords. whereas the planning of CAPTCHA is AN knowledge base topic and also the current collective understanding of this subject continues to be in its infancy, we tend to don't claim that our theme is certainly possible at once. But, as long because the state-of-art-algorithms cannot solve the exhausting AI issues, it's probable to construct a graphical word theme with CAPTCHA that's powerfully immune to spyware.

3. METHODS:

3.1 Graphical Password

A graphical password is easier than a text-based password for most people to remember. Suppose an 8-character password is necessary to gain entry into a particular computer network. Instead of w8KiJ72c, for example, a user might select images of the earth, the country of India, the city of Bhopal, a white stucco house with arched doorways and red tiles on the roof, a green plastic cooler with a white lid, a package of Gouda cheese, a bottle of grape juice, and a pink paper cup with little green stars around its upper edge and three red bands around the middle. Graphical passwords may offer better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words (rather than the recommended jumble of characters). A dictionary search can often hit on a password and allow a hacker to gain entry into a system in seconds. But if a series of selectable images is used on successive screen pages, and if there are many images on each page, a hacker must try every possible

ISSN :2455-0108 Impact Factor : 2015-3.462
IJO–Science
INTERNATIONAL JOURNAL ONLINE OF SCIENCE
Volume II Issue IV July 2016

combination at random. If there are 100 images on each of the 8 pages in an 8-image password, there are 100^8, or 10 quadrillion (10,000,000,000,000,000), possible combinations that could form the graphical password! If the system has a built-in delay of only 0.1 second following the selection of each image until the presentation of the next page, it would take (on average) millions of years to break into the system by hitting it with random image sequences.Graphical password schemes can be grouped into three general categories based on the type of cognitive activity required to remember the password: recognition, recall, and cued recall [5, 12]. Recognition is the easiest for human memory whereas pure recall is most difficult since the information must be accessed from memory with no triggers. Cued recall falls somewhere between these two as it offers a cue which should establish context and trigger the stored memory [12]. Among existing graphical passwords, CCP most closely resembles aspects of Pass faces [9], Story [5], and Pass Points [19, 20]. Therefore these graphical password schemes are presented in more detail. Conceptually, CCP is a blend of the three; in terms of implementation, it is most similar to Pass Points. It also avoids the complex user training requirements found in a number of graphical password proposals, such as that of Weinshall . Pass faces is a graphical password scheme based primarily on recognizing human faces. During password creation, users select a number of images from a larger set. To log in, users must identify one of their pre-selected images from amongst several decoys. Users must correctly respond to a number of these challenges for each login. Davis et al. [5] implemented their own version called Faces and conducted a long-term user study. Results showed that users could accu- Cued Click Points 3 rately remember their images but that user-chosen passwords were predictable to the point of being insecure. Davis et al. [5] proposed an alternative scheme, Story, that used everyday images instead of faces and required that users select their images in the correct order. Users were encouraged to create a story as a memory aid. It fared somewhat worse than Faces for memorability [5], but user choices were much less predictable. The idea of click-based graphical passwords originated with Blonder [2] who proposed a scheme where a password consisted of a series of clicks on prede- fined regions of an image. Later, Wiedenbeck et al. [19, 20] proposed PassPoints, wherein passwords could be composed of several (e.g., 5) points anywhere on an image. They also proposed a “robust discretization” scheme [1], with three overlapping grids, allowing for login attempts that were approximately correct to be accepted and converting the entered password into a cryptographic verification key. Wiedenbeck et al. [19, 20] examined the usability of PassPoints in three separate in-lab user studies to compare text passwords to PassPoints, test whether the choice of image impacted usability, and determine the minimum size of the tolerance square. The overall conclusion was that PassPoints was a usable authentication scheme. We recently conducted two user studies [3] on a PassPoints-style system. Our initial lab study revisited the original usability claims, explored usability of such passwords on a wider range of images (17 images), and gathered information about users’ password choices. Next, we conducted a large-scale field study that examined click-based graphical passwords in practice. Intuitively, it seems obvious that some areas of an image are more attractive to users as click-points [13]. If this phenomenon is too strong, the likelihood that attackers can guess a password significantly increases. If attackers learn which images are being used, they can select a

ISSN :2455-0108 Impact Factor : 2015-3.462
IJO–Science
INTERNATIONAL JOURNAL ONLINE OF SCIENCE
Volume II Issue IV July 2016

set of likely hotspots through image processing tools or by observing a small set of users on the target image and then building an attack dictionary based on those points [6, 16]

3.2 Password Guessing Attack

Password shot attacks will be classified into 2.

Brute Force Attack: it's a kind of positive identification shot attack and consists of attempting each potential mixtures of code, or positive identification till realize the right one. This styles of attack take durable to complete. a posh positive identification will create the time for distinctive the positive identification by brute force long.

Dictionary Attack: Its's another form of positive identification shot attack that uses a wordbook of common words to spot the user's positive identification.

3.3 Shoulder Surfing Attack

Shoulder surfing attack uses direct observation techniques, like wanting over someone's shoulder, to induce info. Shoulder surfboarding is AN economical such the simplest way to induce info in thronged places as a result of it's in need of simple to square next to somebody and appearance out as they fill out a kind, enter a identification number at AN ATM machine. Shoulder surfboarding attack can even be done so much reaching with the help of different vision-enhancing devices. To preclude shoulder surfboarding attack, specialists delegate that you just protect work or your data input device from read by mistreatment your body or bloodletting your hand.

3.4 Captcha

Captcha confide on the separate of capabilities between humans and bots in finding some arduous AI issues. in the main 2 varieties of visual Captcha :

1. Text Captcha
2. Image-Recognition Captcha (IRC).

the previous confide on character identification whereas the latter confide on identification of non-character objects. the subsequent principle has been established:

text Captcha ought to consider the issue of character segmentation, that is computationally valuable and Combinatorially arduous. Machine recognition of non-character objects is much less capable than character recognition. IRCs consider the issue of object identification or classification, probably combined with the issue of object segmentation. Asirra depends on binary object classification: a user is enquired to spot all the hourse from a panel of twelve pictures of Hourse and Cows. Security of IRCs has additionally been studied. Asirra was found to be prone to machine-learning attacks. IRCs based on binary object identification of one concrete form of objects square measure seemingly insecure. Multi-label classification issues square measure considered a lot of more durable than binary classification issues. Captcha may be circumvented through relay attacks whereby Captcha challenges square measure relayed to human solvers, whose answers square measure feedback to the targeted application.

4. CONCLUSION

CaRP, a new security primitive, counting on unsolved hard AI issues. CaRP is both a Captcha and Graphical password pattern. The symbol of CaRP introduce a new group of graphical password espouse a new technique to counter online guess attack. This Captcha pictures is used for every login attempt to create trial of an online guessing attack computationally autonomous of every different.

ISSN :2455-0108 Impact Factor : 2015-3.462
IJO–Science
INTERNATIONAL JOURNAL ONLINE OF SCIENCE
Volume II Issue IV July 2016

5. REFERENCES

[1] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu "Captcha as Graphical Password-A New Security Primitive Based on Hard AI Problems" IEEE Transactions on Information Forensics and Security, Vol.9, No. 6, June 2014

[2] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Compute. Surveys*, vol. 44,no. 4, 2012.

[3] 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.

[4] Robert G. Rittenhouse, Junaid Ahsenali Chaudry and Malrey Lee, "Security in Graphical Authentication", International Journal of Security and Its Application Vol. , No. 3,, Ma, 2013

[5] Susan Wiedenbecka, Jim Watersa, Jean-Camille Birgetb,Alex Brodskiyc, Nasir Memon,"PassPoints: Design and longitudinal evaluation of a graphical password system", Int. J.HCI, Vol. 63, pp. 102-127, July 2005.

[6] H. Gao, X. Liu, S.Wang, and R. Dai, "A new graphical password scheme against spyware by using CAPTCHA," in *Proc. Symp. Usable Privacy Security*, 2009, pp. 760–767.

[7] J. Yan, A. Blackwell, R. Anderson, and A. Grant, The Memorability and Security of Passwords – Some Empirical Results, Technical Report, no. 500, Com-puter Laboratory, University of Cambridge, 2000.

[8] D. Weinshall. Cognitive Authentication Schemes Safe Against Spyware. In Symposium on Security and Privacy,2006

[9] B. Pinkas , and T. Sander. Securing passwords against dictionary attacks. In Proceedings of the ACM Computer and Security Conference, 2002, pp.161–170.

[10] J. Yan, "A note on proactive password checking,"ACM New Security Paradigms Workshop, pp. 127–135, New Mexico, USA, 2001.

[11] L. Sobrado, and J. Birget, Graphical Passwords, The Rutgers Scholar, Rutgers University, Camden New Jersey 081024, 2002.

[12] A. Perrig, and D. Song, "Hash visualization: A new technique to improve real-world security," Interna- tional Workshop on Cryptographic Techniques and E-ommerce, pp. 131-138, 1999.

[13] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin. The design and analysis of graphical passwords. In 8th USENIX Security Symposium, August 1999.

[14] M. Orozco, B. Malek, M. Eid, and A. El Saddik. Haptic-based sensible graphical password. In Proceedings of Virtual Concept, 2006.

[15] A. Paivio. Mind and Its Evolution: A Dual Coding Theoretical Approach. Lawrence Erlbaum: Mahwah, N.J., 2006.

[16] D. Nali, and J. Thorpe, Analyzing User Choice In Graphical Passwords, Technical Report TR-04-01, Carleton University, Canada, 2004.

[17] J. Thorpe and P. C. van Oorschot. Graphical dictionaries and the memorable space of graphical passwords. In 13th USENIX Security Symposium, August 2004.

ISSN :2455-0108 Impact Factor : 2015-3.462
IJO–Science
INTERNATIONAL JOURNAL ONLINE OF SCIENCE
Volume II Issue IV July 2016

[18] J. Thorpe. On the Predictability and Security of User Choice in Passwords. PhD thesis, School of Computer

Science, Carleton University, January 2008.

[19] J. Thames, R. Abler, and D. Keeling. A distributed active response architecture for preventing SSH dictionary attacks. In IEEE Southeastcon, 2008.

[20] F. Tari, A. Ozok, and S. Holden. A comparison of perceived and real shoulder-sur_ng risks between alphanumeric and graphical passwords. In 2nd ACM Symposium on Usable Privacy and Security (SOUPS), 2006.

[21] H. Tao and C. Adams. Pass-Go: A proposal to improve the usability of graphical passwords. International Journal of Network Security, 7(2):273, 292, 2008.

[22] H. Tao. Pass-Go, a new graphical password scheme. Master's thesis, School of Information Technology and Engineering, University of Ottawa, June 2006.

[23] A. Salehi-Abari, J. Thorpe, and P. van Oorschot. On purely automated attacks and click-based graphical passwords. In Annual Computer Security Applications Conf. (ACSAC), 2008.