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

Graphical Passwords for Artificial Intelligence Problems

Mohammad Asif
Pursuing M.Tech,
Department of Computer Science,
Ganapathi Engineering College, Warangal.

A.Prathap Reddy
Head of the Department,
Department of Computer Science,
Ganapathi Engineering College, Warangal.

Abstract: :

Artificial Intelligence is predominant in all technologies. But this artificial intelligence is used for anti-social activities by the hackers and intruders of cybercrime. Using the artificial intelligence the criminals are breaking the passwords of financial applications of the users and eavesdrop the valuable information. The usage of artificial intelligence in breaking the passwords of financial applications with the guessing attacks has become a threat in cybercrime. To arrest these problems arise from the artificial intelligence we introduce a novel concept of image passwords. Usage of image passwords along with log in information in the financial data application log in screens can solve the problems of the guessing attacks with the help of Artificial Intelligence. To introduce this graphical passwords a novel Captcha technology has been implemented in this project. This technology has provided reasonable security to prevent guessing attacks of the cyber criminals.

Keywords:

Graphical Password, Captcha, guessing attack, Security implementations.

1.INTRODUCTION:

The security implementations in the web based applications can be possible with the help of cryptographic primitives. But the security implementation with the help of cryptosystems are broken by cyber criminals and using artificial intelligence to intrude into the applications. The digital signature algorithms have been introduced to overcome these problems. But these are also become in vain before the power of execution of artificial intelligence. To admeasure the problems encountered by Artificial Intelligence to break the passwords with guessing attacks a novel primitive has been invented in the form of Captcha. This Captcha is used by the humans with great ease but it is difficult for computers or any artificial intelligence software.

Captcha is a novel method to stop the problems incurred by the Artificial Intelligence. Captcha technology is rich with some text material in a prescribed area and it is supported by a key which regenerate another Captcha to be typed by the human beings. However, this new paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications. Is it possible to create any new security primitive based on hard AI problems? This is a challenging and interesting open problem. In this paper, we introduce a new security primitive based on hard AI problems, namely, a novel family of graphical password systems integrating Captcha technology, which we call CaRP (Captcha as gRaphical Passwords). CaRP is click-based graphical passwords, where a sequence of clicks on an image is used to derive a password. Unlike other click-based graphical passwords, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every login attempt.

The notion of CaRP is simple but generic. CaRP can have multiple instantiations. In theory, any Captcha scheme relying on multiple-object classification can be converted to a CaRP scheme. We present exemplary CaRPs built on both text Captcha and image-recognition Captcha. One of them is a text CaRP wherein a password is a sequence of characters like a text password, but entered by clicking the right character sequence on CaRP images.CaRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services. This threat is widespread and considered as a top cyber security risk. Defense against online dictionary attacks is a more subtle problem than it might appear. Intuitive countermeasures such as throttling logon attempts do not work well for two reasons:

1) It causes denial-of-service attacks (which were exploited to lock highest bidders out in final minutes of eBay auctions [12]) and incurs expensive helpdesk costs for account reactivation..
2) It is vulnerable to global password attacks whereby adversaries intend to break into any account rather than

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

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 offers protection against relay attacks, an increasing threat to bypass Captchas protection, wherein Captcha challenges are relayed to humans to solve. Koobface was a relay attack to bypass Facebook's Captcha in creating new accounts. CaRP is robust to shoulder-surfing attacks if combined with dual-view technologies.CaRP requires solving a Captcha challenge in every login. This impact on usability can be mitigated by adapting the CaRP image's difficulty level based on the login history of the account and the machine used to log in. Typical application scenarios for CaRP include:

1) CaRP can be applied on touch-screen devices whereon typing passwords is cumbersome, esp. for secure Internet applications such as e-banks. Many e-banking systems have applied Captchas in user logins [39]. For example,ICBC (www.icbc.com.cn), the largest bank in the world,requires solving a Captcha challenge for every online login attempt.

2) CaRP increases spammer's operating cost and thus helps reduce spam emails. For an email service provider that deploys CaRP, a spam bot cannot log into an email account even if it knows the password. Instead,human involvement is compulsory to access an account.

If CaRP is combined with a policy to throttle the numberof emails sent to new recipients per login session, a spam bot can send only a limited number of emails before asking human assistance for login, leading to reduced outbound spam traffic.The remaining paper is organized as follows: Background and related work are presented in Section II. We outline CaRP in Section III, and present a variety of CaRP schemes in Sections IV and V. Security analysis is provided in Section VI. A usability study on two CaRP schemes that we have implemented is reported in Section VII. Balance of security and usability is discussed in Section VIII. We conclude the paper with Section IX.

II. BACKGROUND AND RELATED WORK:

A. Graphical Passwords:

A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI).

For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA).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 (from among a screen full of real and fictitious planets), the country of France (from a map of the world), the city of Nice (from a map of France), 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 combination at random. If there are 100 images on each of the 8 pages in an 8-image password, there are 1008, 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.

2.Captcha Mechanism:

A CAPTCHA (an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart") is a type of challenge-response test used in computing to determine whether or not the user is human. The term was coined in 2003 by Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford.[1] The most common type of CAPTCHA was first invented in 1997 by Mark D. Lillibridge, Martin Abadi, Krishna Bharat, and Andrei Z. Broder. This form of CAPTCHA requires that the user type the letters of a distorted image, sometimes with the addition of an obscured sequence of letters or digits that appears on the screen. Because the test is administered by a computer, in contrast to the standard Turing test that is administered by a human, a CAPTCHA is sometimes described as a reverse Turing test.

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

This term is ambiguous because it could also mean a Turing test in which the participants are both attempting to prove they are the computer.This user identification procedure has received many criticisms, especially from disabled people, but also from other people who feel that their everyday work is slowed down by distorted words that are illegible even for users with no disabilities at all.

3.Authentication mechanism through Captcha:

With the demonstration (through research publications) that character recognition CAPTCHAs are vulnerable to computer vision based attacks, some researchers have proposed alternatives to character recognition, in the form of image recognition CAPTCHAs which require users to identify simple objects in the images presented. The argument is that object recognition is typically considered a more challenging problem than character recognition, due to the limited domain of characters and digits in the English alphabet.

Some proposed image recognition CAPTCHAs include:

Chew et al. published their work in the 7th International Information Security Conference, ISC'04, proposing three different versions of image recognition CAPTCHAs, and validating the proposal with user studies. It is suggested that one of the versions, the anomaly CAPTCHA, is best with 100% of human users being able to pass an anomaly CAPTCHA with at least 90% probability in 42 seconds. [24]Datta et al. published their paper in the ACM Multimedia '05 Conference, named IMAGINATION (IMAge Generation for INternetAuthenticaTION), proposing a systematic way to image recognition CAPTCHAs. Images are distorted in such a way that state-of-the-art image recognition approaches (which are potential attack technologies) fail to recognize them.[25]Microsoft (Jeremy Elson, John R. Douceur, Jon Howell, and Jared Saul) have developed Animal Species Image Recognition for Restricting Access (ASIRRA) which ask users to distinguish cats from dogs. Microsoft had a beta version of this for websites to use.[26] They claim "Asirra is easy for users; it can be solved by humans 99.6% of the time in under 30 seconds. Anecdotally, users seemed to find the experience of using Asirra much more enjoyable than a text-based CAPTCHA."

This solution was described in a 2007 paper to Proceedings of 14th ACM Conference on Computer and Communications Security (CCSIts) [27] However, this project was closed in October 2014 and is no longer available. CAPTCHAs based on reading text — or other visual-perception tasks — prevent blind or visually impaired users from accessing the protected resource.[7] However, CAPTCHAs do not have to be visual. Any hard artificial intelligence problem, such as speech recognition, can be used as the basis of a CAPTCHA. Some implementations of CAPTCHAs permit users to opt for an audio CAPTCHA.[8] Other implementations do not require users to enter text, instead asking the user to pick images with common themes from a random selection.[9] For non-sighted users (for example blind users, or the color blind on a color-using test), visual CAPTCHAs present serious problems. Because CAPTCHAs are designed to be unreadable by machines, common assistive technology tools such as screen readers cannot interpret them. Since sites may use CAPTCHAs as part of the initial registration process, or even every login, this challenge can completely block access. In certain jurisdictions, site owners could become target of litigation if they are using CAPTCHAs that discriminate against certain people with disabilities. For example, a CAPTCHA may make a site incompatible with Section 508 in the United States. In other cases, those with sight difficulties can choose to identify a word being read to them.

While providing an audio CAPTCHA allows blind users to read the text, it still hinders those who are both visually and hearing impaired. According to sense.org.uk, about 4% of people over 60 in the UK have both vision and hearing impairments. There are about 23,000 people in the UK who have serious vision and hearing impairments. According to The National Technical Assistance Consortium for Children and Young Adults Who Are Deaf-Blind (NTAC), the number of deafblind children in the USA increased from 9,516 to 10,471 during the period 2004 to 2012.[10] Gallaudet University quotes 1980 to 2007 estimates which suggest upwards of 35,000 fully deafblind adults in the USA.[11] Deafblind population estimates depend heavily on the degree of impairment used in the definition.The use of CAPTCHA thus excludes a small number of individuals from using significant subsets of such common Web-based services as PayPal, GMail, Orkut, Yahoo!, many forum and weblog systems, etc. Even for perfectly sighted individuals, new generations of graphical CAPTCHAs, designed to overcome sophis

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

ticated recognition software, can be very hard or impossible to read.A method of improving the CAPTCHA to ease the work with it was proposed by ProtectWebForm and was called "Smart CAPTCHA".[12] Developers advise to combine the CAPTCHA with JavaScript support. Since it is too hard for most of spam robots to parse and execute JavaScript, using a simple script which fills the CAPTCHA fields and hides the image and the field from human eyes was proposed.

GRAPHICAL PASSWORDS FROM CAPTCHA:

In a guessing attack, a password guess tested in an unsuccessfultrial is determined wrong and excluded from subsequenttrials. The number of undetermined password guessesdecreases with more trials, leading to a better chance of findingthe password. Mathematically, let Sbe the set of passwordguesses before any trial, ρ be the password to find, T denote a trial whereas Tndenote the n-th trial, and p(T = ρ) bethe probability that ρ is tested in trial T. Let En be the setof password guesses tested in trials up to (including) Tn. Thepassword guess to be tested in n-th trial Tnis from set S\En−1, i.e., the relative complement of En−1 in S. If ρ S, then we have

p(T = ρ|T1 _= ρ, . . . , Tn−1 _= ρ) >p(T = ρ), (1)
andEn →S
p(T = ρ|T1 _= ρ, . . . , Tn−1 _= ρ) →1 _

withn → |S|, (2)where |S| denotes the cardinality of S. From Eq. (2), thepassword is always found within |S| trials if it is in S; otherwise S is exhausted after |S| trials. Each trial determines if the tested password guess is the actual password or not, andthe trial's result 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 thusRequire more trials. No matter how secure a graphical passwordscheme is, the password can always be found by a brute forceattack. In this paper, we distinguish two types of guessingattacks: automatic guessing attacks apply an automatic trialand error process but S can be manually constructed whereashuman guessing attacks apply a manual trial and error process.CaRP adopts a completely different approach to counterautomatic guessing attacks. It aims at realizing the followingequation:p(T = ρ|T1, . . . , Tn−1) = p(T = ρ), n (3)

in an automatic guessing attack. Eq. (3) means that each trialis computationally independent of other trials. Specifically,no matter how many trials executed previously, the chanceof finding the password in the current trial always remainsthe same. That is, a password in S can be found onlyprobabilisticallyby automatic guessing (including brute-force)attacks, in contrast to existing graphical password schemesWhere a password can be found within a fixed number of trials.How to achieve the goal? If a new image is used for eachtrial, and images of different trials are independent of eachother, then Eq. (3) holds. Independent images among differentlogin attempts must contain invariant information so that theauthentication server can verify claimants.

By examining theecosystem of user authentication, we noticed that human usersenter passwords during authentication, whereas the trial anderror process in guessing attacks is executed automatically.The capability gap between humans and machines can be exploited to generate images so that they are computationallyindependentyet retain invariants that only humans can identify,and thus use as passwords. The invariants among imagesmust be intractable to machines to thwart automatic guessingattacks. This requirement is the same as that of an idealCaptcha [25], leading to creation of CaRP, a new family ofgraphical passwords robust to online guessing attacks.

Converting Captcha to CaRP:

In principle, any visual Captcha scheme relying on recognizingtwo or more predefined types of objects can be convertedto a CaRP. All text Captcha schemes and most IRCs meet thisrequirement. Those IRCs that rely on recognizing a singlepredefined type of objects can also be converted to CaRPsin general by adding more types of objects. In practice,conversion of a specific Captcha scheme to a CaRP schemetypically requires a case by case study, in order to ensureboth security and usability.

We will present in Sections IVand V several CaRPs built on top of text and image-recognitionCaptcha schemes. Some IRCs rely on identifying objects whose types are notpredefined. A typical example is Cortcha [25] which relieson context-based object recognition wherein the object to berecognized can be of any type. These IRCs cannot be convertedinto CaRP since a set of pre-defined object types is essential for constructing a password.

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

D. User Authentication With CaRP Schemes:

Like other graphical passwords, we assume that CaRP-schemes are used with additional protection such as securechannels between clients and the authentication server throughTransport Layer Security (TLS). A typical way to apply CaRP schemes in user authentication is as follows. The authenticationserver AS stores a salt s and a hash value H(ρ, s) foreach user ID, where ρ is the password of the account andnot stored. A CaRP password is a sequence of visual objectIDs or clickable-points of visual objects that the user selects. Upon receiving a login request, AS generates a CaRP image, records the locations of the objects in the image, and sendsthe image to the user to click her password. The coordinatesof the clicked points are recorded and sent to AS along

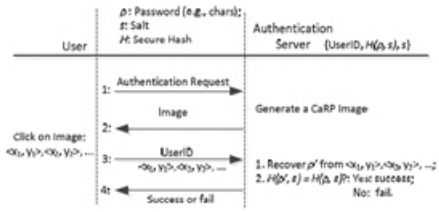


Fig. 1.Flowchart of basic CaRP authentication

with the user ID. AS maps the received coordinates onto theCaRP image, and recovers a sequence of visual object IDs orclickable points of visual objects, ρ_, that the user clicked onthe image. Then AS retrieves salt s of the account, calculatesthe hash value of ρ_ with the salt, and compares the resultwith the hash value stored for the account.Authenticationsucceeds only if the two hash values match. This process iscalled the basic CaRP authentication and shown in Fig. 1.Advanced authentication with CaRP, for example,

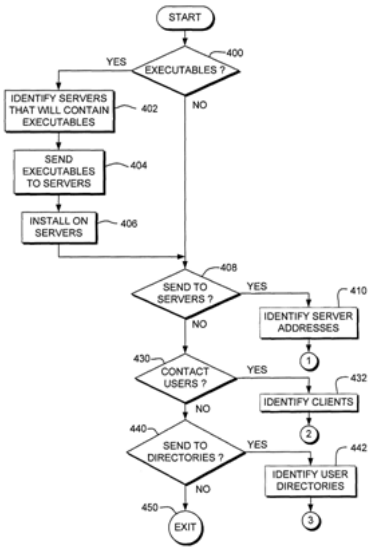
Challenge-response will be presented in Section V-B. Weassume in the following that CaRP is used with the basicCaRP authentication unless explicitly stated otherwise. To recover a password successfully, each user-clicked pointmust belong to a single object or a clickable-point of anobject. Objects in a CaRP image may overlap slightly withneighboring objects to resist segmentation. Users should notclick inside an overlapping region to avoid ambiguity inidentifying the clicked object. This is not a usability concern inpractice since overlapping areas generally take a tiny portionof an object.

THE PREDOMINANT PART OF THE PROJECT:

The CaRP is designed with a sequence of visual objects. Per view of traditional recognitionbased graphical passwords, recognition-based CaRP seems to have access to an infinite number of different visual objects. We present recognition-based CaRP schemes and a variation next.A password is a sequence of clickable points. A character can typically contribute multiple clickable points. Therefore TextPoints has a much larger password space than ClickText. 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.



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

It is worth comparing potential password points between TextPoints and traditional click-based graphical passwords such as PassPoints [5]. In PassPoints, salient points should be avoided since they are readily picked up by adversaries to mount dictionary attacks, but avoiding salient points would increase the burden to remember a password. This conflict does not exist in TextPoints. 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.

CRITICAL EVALUATION:

Guessing attacks predominantly affected the business of B2B. The financial transactions of the banks should be kept online. So that the business of the banks will get improved. To keep the financial transactions a strong online security mechanism should be developed. The need of a security mechanism for financial transactions conducted by the financial institutions is very high. The security mechanism should act against the guessing attacks. Guessing attacks are more powerful and breaking the passwords of the online financial transactions and stealing the data. The present proposed project is development of a security mechanism against the guessing attacks. The proposed project is also creating a security layer for the financial transactions and obstructs the intruders into the financial online applications.The research studies revealed that the investigations have done and found a admeasure with the password security. The mechanism has run for a period until the hackers started to break these passwords with their creative mechanism. Then the researchers have developed the advanced encryption standards against the hackers' attacks. Those increased security mechanism have not endure much time in protecting the web applications.

SECURITY IMPLEMENTATION:

Computational intractability in recognizing objects in CaRP images is fundamental to CaRP. Existing analyses on Captcha security were mostly case by case or used an approximate process. No theoretic security model has been established yet. Object segmentation is considered as a computationallyexpensive, combinatorially-hard problem [30], which modern text Captcha schemes rely on. According to [30], the complexity of object segmentation, C, is exponentially dependent of the number M of objects contained in a challenge, and polynomially dependent of the size N of the Captcha alphabet: $C = \alpha M P(N)$, where $\alpha > 1$ is a parameter, and P() is a polynomial function. A Captcha challenge typically contains 6 to 10 characters, whereas a CaRP image typically contains30 or more characters. The complexity to break a Click- Text image is about $\alpha 30P(N)/(\alpha 10P(N)) = \alpha 20$ times the complexity to break a Captcha challenge generated by its underlying Captcha scheme. Therefore ClickText is much harder to break than its underlying Captcha scheme. Furthermore, characters in a CaRP scheme are arranged twodimensionally, further increasing segmentation difficulty due to one more dimension to segment. As a result, we can reduce distortions in ClickText images for improved usability yet maintain the same security level as the underlying text Captcha.

EXPERIMENTAL RESULTS:

Usability. Among all the recorded login attempts, 24.4% failed. Tests after a larger interval tended to have more failed attempts. Some participants contributed significantly more failed attempts than others. At the end of tests, 40 (100%) participants remembered their PassPoints passwords, 39 (97.5%) remembered their passwords of both ClickText and AnimalGrid, and 34 (85%) remembered their Text passwords. One participant forgot the AnimalGrid password at the onehour test, and another one forgot the ClickText password at the one-week test. For Text, two participants forgot their passwords at the one-week test, and four forgot at the threeweek test. PassPoints scored the best in memorability whereas Text scored the worst. This may be partially due to the fact that hotspots were allowed for PassPoints passwords, and that Text passwords had a much larger alphabet than both ClickText and AnimalGrid.

CONCLUSION:

The revolutionary experimental research work has been done in incorporating the security with encrypted mechanism.

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

The revolutionary changes and innovative changes have been doneThe digital encryption standards have been deployed to hide the real password of the user and tried to protect the interest of online financial application users. All the trails have become in vain. Even digital encrypted textual passwords also decrypted with the wise characteristics of hackers and intruders. The hackers again started looting the valuable data of the financial organizations. The hackers and attackers have adopted sophisticated cracking techniques for textual passwords and intrude into the applications and caused irrevocable damage to the application storing data.Overall, our work is one step forward in the paradigm of using hard AI problems for security. Of reasonable security and usability and practical applications, CaRP has good potential for refinements, which call for useful future work. More importantly, we expect CaRP to inspire new inventions of such AI based security primitives.

REFERENCES:

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

[2](2012, Feb.). The Science Behind Passfaces [Online]. Available:http://www.realuser.com/published/ScienceBehindPassfaces.pdf

[3]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.

[6]P. C. van Oorschot and J. Thorpe, "On predictive models and userdrawn graphical passwords," ACM Trans. Inf. Syst. Security, vol. 10,no. 4, pp. 1–33, 2008.

[7]K. Golofit, "Click passwords under investigation," in Proc. ESORICS, 2007, pp. 343–358.

[8]A. E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the passpoints graphical password scheme," in Proc. Symp. Usable 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 automatedattacks 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/

[13]HP TippingPointDVLabs, 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.

[16]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.

[17]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.

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

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

[19]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.

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

[21]R. Dhamija and A. Perrig, "Déjà Vu: A user study using images forauthentication," in Proc. 9th USENIX Security, 2000, pp. 1–4.

[22]D. Weinshall, "Cognitive authentication schemes safe against spyware," in Proc. IEEE Symp. Security Privacy, May 2006, pp. 300–306.

[23]P. Dunphy and J. Yan, "Do background images improve 'Draw a Secret'graphical passwords," in Proc. ACM CCS, 2007, pp. 1–12.[24] P. Golle, "Machine learning attacks against the Asirra CAPTCHA," inProc. ACM CCS, 2008, pp. 535–542.

[24]B. B. Zhu et al., "Attacks and design of image recognition CAPTCHAs,"in Proc. ACM CCS, 2010, pp. 187–200.

[25]J. Yan and A. S. El Ahmad, "A low-cost attack on a microsoftCAPTCHA," in Proc. ACM CCS, 2008, pp. 543–554.

[26]G. Mori and J. Malik, "Recognizing objects in adversarial clutter," in Proc. IEEE Comput. Society Conf. Comput. Vis. Pattern Recognit.,Jun. 2003, pp. 134–141.

[27]G. Moy, N. Jones, C. Harkless, and R. Potter, "Distortion estimation techniques in solving visual CAPTCHAs," in Proc. IEEE Comput. Soc.Conf. Comput. Vis. Pattern Recognit., Jul. 2004, pp. 23–28.

[28]K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski, "Computers beat humans at single character recognition in reading-based human interaction proofs," in Proc. 2nd Conf. Email Anti-Spam, 2005, pp. 1–3.

[29]K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski, "Building segmentation based human-friendly human interaction proofs," in Proc.2nd Int. Workshop Human Interaction Proofs, 2005, pp. 1–10.

[30]J. Elson, J. R. Douceur, J. Howell, and J. Saul, "Asirra: A CAPTCHA that exploits interest-aligned manual image categorization," in Proc. ACM CCS, 2007, pp. 366–374.

[31]R. Lin, S.-Y. Huang, G. B. Bell, and Y.-K. Lee, "A new CAPTCHA interface design for mobile devices," in Proc. 12th Austral. User Inter.Conf., 2011, pp. 3–8.