e-ISSN: 2349-9745
p-ISSN: 2393-8161
Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Captcha as Graphical Passwords with Click Text and Animal Grid Session Password

PRIYANKA.S[1], Ms.NITHYA .S[2]
[1]M.E.Communication Systems student, [2]Assistant professor, Department of ECE,
[1,2]DhanalakshmiSrinivasan Engineering College,Perambalur

Abstract-Textual passwords are the most common method used for authentication. But textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing. New security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme. CaRP also offers a novel approach to address the well-known image hotspot problem in popular graphical password systems, such as Pass Points, 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 and also implement for Text can be combined with images or colors to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated. The two techniques are proposed to generate session passwords using text and colours which are resistant to shoulder surfing. These methods are suitable for Personal Digital Assistants and also implement for PGRP protocol for prevent the any vulnerable attackers.

Index Terms—Graphical password, password, CaRP, Captcha, dictionary attack, password guessing attack, ATT, DAS.

I. INTRODUCTION

A FUNDAMENTAL task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. For example, the problem of integer factorization is fundamental to the RSA public-key cryptosystem and the Rabin encryption. The discrete logarithm problem is fundamental to the ElGamal encryption, the Diffie- Hellman key exchange, the Digital Signature Algorithm, the elliptic curve cryptography and so on.

Using hard AI (Artificial Intelligence) problems for security, initially proposed in is an exciting new paradigm. Under this paradigm, the most notable primitive invented is Captcha, which distinguishes human users from computers by presenting a challenge, i.e., a puzzle, beyond the capability of computers but easy for humans. Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots.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 Defence against online dictionary attacks is a more subtle problem than it might appear. Intuitive counter measures such as throttling logon attempts do not work well for two reasons:
1) It causes denial-of-service attacks
2) It is vulnerable to global password attacks 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 offers protection against relay attacks, an increasing threat to bypass Captchas protection, wherein Captcha challenges are relayed to humans to solve.. CaRP is robust to shoulder-surfing attacks if combined with dual-view technologies.
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 Captcha as in user logins. 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

II. SECURITY

An authentication system must provide adequate security for its intended environment, otherwise it fails to meet its primary goal. A proposed system should at minimum be evaluated against common attacks to determine it satisfies security requirements. We classify the types of attacks on knowledge-based authentication into two general categories: guessing and capture attacks. In successful guessing attacks, attackers are able to either exhaustively search through the entire theoretical password space, or predict higher probability passwords (i.e., create a dictionary of likely passwords) so as to obtain an acceptable success rate within a manageable number of guesses.

Guessing attacks may be conducted online through the intended login interface or offline if someveriable text can be used to assess the correctness of guesses. Authentication systems with small theoretical password spaces or with identi_able patterns in user choice of passwords are especially vulnerable to guessing attacks.

Password capture attacks involve directly obtaining the password, or part thereof, by capturing login when entered by the user, or by tricking the user into valuing their password. Shoulder surfing, phishing, and some kinds of malware are common forms of capture attacks.In shoulder-surfing, credentials are captured by direct observation of the login process or through some external recording device such as a video camera. Phishing is a type of social engineering where users are tricked into entering their credentials at a fraudulent website recording user input.

III. EXISTING SYSTEM

Brute force and dictionary attacks on password-only remote login services Existing techniques and proposals involve ATTs, with the underlying assumption that these challenges are sufficiently difficult for bots and easy for most people. However, users increasingly dislike ATTs as these are perceived as an extra step; for usability issues related to commonly used CAPTCHAs.

Attackers can try only limited number of guesses from a single machine before being locked- out, delayed, or challenged to answer Automated Turing Tests (ATTs, e.g., CAPTCHA).

Account locking is a customary mechanism to prevent an adversary from attempting multiple passwords for a particular username. Although locking is generally temporary, the adversary can mount a DoS attack by making enough failed login attempts to lock a particular account. Delaying server response after receiving user credentials, whether the password is correct or incorrect, prevents the adversary from attempting a large number of passwords in a reasonable amount of time for a particular username. Traditional password-based authentication is not suitable for any UN trusted environment (e.g., a key logger may record all keystrokes, including passwords in a system, and forward those to a remote attacker). We do not prevent existing such attacks in un trusted environments, and thus essentially assume any machines that legitimate users use for login are trustworthy

In this project, a graphical password system with a supportive sound signature to in the existing system, Blonder-style passwords are based on cued recall. A user clicks on several previously chosen locations in a single image to log in. As implemented by Pass logic Corporation, the user chooses several predefined regions in an image as his or her password. To log in the user has to click on the same regions in effect, cued click points (ccp) is a proposed alternative to pass points. In ccp, users click one point on each of 5 images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point. It also makes attacks based on hotspot analysis more challenging. Each click results in showing a next-image, in Effect leading users down a "path" as they click on their sequence of points.

1. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click.
2. Users can choose their images only to the extent that their click-point dictates the next image. While the predictability problem can be solved by disallowing user choice and assigning passwords to users, this usually leads to usability issues since users cannot easily remember such random passwords.
3. Number of graphical password systems have been developed, Study shows that text-based passwords suffers with both security and usability problems

A. Graphical Passwords

A large number of graphical password schemes have been proposed. They can be classified into three categories according to the task involved in memorizing and entering passwords: recognition, recall, and cued recall. Each type will be briefly described here. More can be found in a recent review of graphical passwords.

A *recognition-based* scheme requires identifying among decoys the visual objects belonging to a password portfolio. A typical scheme is Pass faces wherein a user selects a portfolio of faces from a database in creating a password. During authentication, a panel of candidate faces is presented for the user to select the face belonging to her portfolio. This process is repeated several rounds, each round with a different panel. A successful login requires correct selection in each round. The set of images in a panel remains the same between logins, but their locations are permuted. Story is similar to pass faces but the images in the portfolio are ordered, and a user must identify her portfolio images in the correct order. Déjà Vu is also similar but uses a large set of computer generated "random-art" images. Cognitive Authentication requires a user to generate a path through a panel of images as follows: starting from the top-left image, moving down if the image is in her portfolio, or right otherwise.

This process is repeated, each time with a different panel. A successful login 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) was the first recall-based scheme proposed. A user draws her password on a 2D grid.

In a ***cued-recall*** scheme, an external cue is provided to help memorize and enter a password. Pass Points is a widely studied click-based cued-recall scheme wherein a user clicks a sequence of points anywhere on an image in creating a password, and re-clicks the same sequence during authentication. Cued Click Points (CCP) is similar to Pass Points but uses one image per click, with the next image selected by a deterministic function. Persuasive Cued Click Points (PCCP) 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, recognition is considered the easiest for human memory whereas pure recall is the hardest. Recognition is typically the weakest in resisting guessing attacks. Many proposed recognition-based schemes practically have a password space in the range of 213 to 216 passwords. A study reported that a significant portion of passwords of DAS and Pass-Go were successfully broken with guessing attacks using dictionaries of 231 to 241 entries, as compared to the full password space of 258 entries. Hotspots were exploited to mount successful guessing attacks on Pass Points a significant portion of passwords were broken with dictionaries of 226 to 235 entries, as compared to the full space of 243 passwords.

B.Captcha

Captcha relies on the gap of capabilities between humans and bots in solving certain hard AI problems. There are two types of visual Captcha: text Captcha and Image-Recognition Captcha (IRC). The former relies on character recognition while the latter relies on recognition of non-character objects. Security of text Captchas has been extensively studied. The following principle has been established: text Captcha should rely on the difficulty of character segmentation, which is computationally expensive and combinatorial hard .Machine recognition of non-character objects is far less capable than character recognition.

Architecture of Existing System

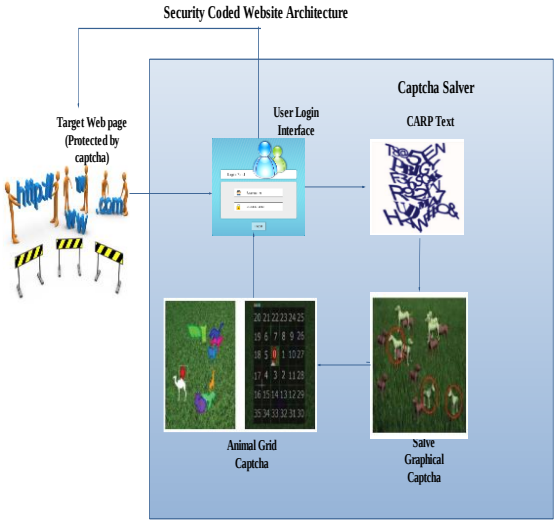

Figure 1. Architecture of existing system

IV. PROPOSED SYSTEM

A password is a sequence of some invariant points of objects. An *invariant point* of anobject (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 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. Text Point, a recognition recall CaRP scheme with an alphabet of characters, is presented next, followed by a variation for challenge response authentication.

Text Points

Characters contain invariant points. 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 Text Points. The internality ensures that a clickable point is unlikely occluded by a neighbouring character and that its tolerance region unlikely overlaps with any tolerance region of a neighbouring 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. In addition, variation should also be taken into consideration. For example, if the centre of a stroke segment in one character is selected, we should avoid selecting the centre of a similar stroke segment in another character. Instead, we should select a different point from the stroke segment, e.g., a point at one-third length of the stroke segment to an end. This variation in selecting clickable points ensures that a clickable point is context-dependent: a similarly structured point may or may not be a clickable point, depending on the character that the point lies in. Character recognition is required in locating clickable points on a Text Points image although the clickable points are known for each character. This is a task beyond a boot's capability.

Click Text

Click Text 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" 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 Click Text 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... In Click Text images, characters can be arranged randomly on 2D space. This is different from text Captcha challenges in which characters are typically ordered from left to right in order for users to type them sequentially. Click Text image with an alphabet of 33 characters. In entering a password, the user clicks on this image the characters in her password, in the same order, for example "A", "B", "#", "9", "C","D","8",andthen"7"for password ρ="AB#9CD87".

Figure 2. Click text

Click Animal

Captcha Zoo is a Captcha scheme which uses 3D models of horse and dog to generate 2D animals with different textures, colours, lightings and poses, and arranges them on a cluttered background. A user clicks all the horses in a challenge image to pass the test. Shows a sample challenge wherein all the horses are circled red. *Click Animal* is a recognition-based CaRP scheme built on top of Captcha Zoo, 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 Click Animal images: 3D models are used to generate 2D animals by applying different views, textures, colours, lightning effects, and optionally distortions. 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. . Note that different views applied in mapping 3D models to 2D animals, together with occlusion in the following step, produce many different shapes for the same animal's instantiations in the generated images. Combined with the additional anti-recognition mechanisms applied in the mapping step, these make it hard for computers to recognize animals in the generated image, yet humans can easily identify different instantiations of animals

Figure 3. Click animal

Animal Grid

The number of similar animals is much less than the number of available characters. Click Animal has a smaller alphabet, and thus a smaller password space, than Click Text. CaRP should have a sufficiently-large effective password space to resist human guessing attacks.

DAS is a candidate but requires drawing on the grid. To be consistent with Click Animal, we change from drawing to clicking: *Click-A-Secret (CAS)* wherein a user clicks the grid cells in her password. *Animal Grid* is a combination of Click Animal 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 labelled grid-cell of the wrong grid would likely produce a wrong grid-cell at the authentication server side when the correct grid is used. To enter a password, a Click Animal image is displayed first.

After an animal is selected, an image of $n \times n$ grid appears, with the grid-cell size equalling the bounding rectangle of the selected animal. Each grid-cell is labelled to help users identify. Therefore a password is a sequence of animals interleaving with grid-cells, e.g., ρ = "Dog, Grid_2_, Grid_1_; Cat, Horse, Grid_3_", where Grid_1_ means the grid-cell indexed as 1, and grid-cells after an animal means that the grid is determined by the bounding rectangle of the animal. A password must begin with an animal. When a Click Animal image appears, the user clicks the animal on the image that matches the first animal in her password. The coordinates of the clicked point are recorded. The bounding rectangle of the clicked animal is then found interactively as follows: a bounding rectangle is calculated and displayed. The user checks the displayed rectangle and corrects inaccurate edges by dragging if needed. This process is repeated until the user is satisfied with the accuracy of the bounding rectangle. In most cases, the calculated bounding rectangle is accurate enough without needing manual correction

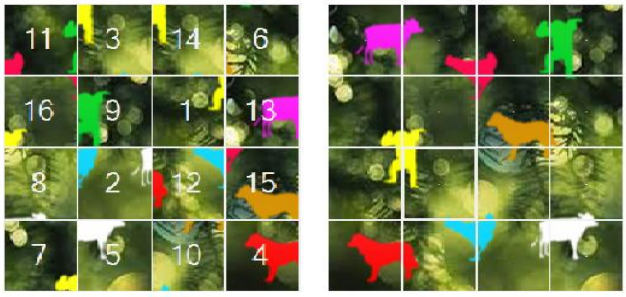

Figure 4.Animal Grid

PGRP Protocol

The proposed PGRP scheme is more restrictive against attackers than commonly used countermeasures. At the same time, PGRP requires answering fewer ATTs for all legitimate users, including those who occasionally require multiple attempts to recall a password. Presented a login protocol based on ATTs to protect against online password guessing attacks. It reduces the number of ATTs that legitimate users must correctly answer so that a user with a valid browser cookie will rarely be prompted to answer an ATT.

A deterministic function (AskATT) of the entered user credentials is used to decide whether to ask the user an ATT. To improve the security of the PS protocol, A secure non-deterministic keyed hash function as AskATT() so that each username is associated with one key that should be changed whenever the corresponding password is changed. The proposed function requires extra server-side storage per username and at least one cryptographic hash operation per login attempt. In the proposed work we have integrated sound signature to help in recalling the password. In daily life we see various examples of recalling an object by the sound related to that object enters User ID and select one sound frequency which he want to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter.

V. PROTOCOL GOALS

1. The login protocol should make brute force and dictionary attacks ineffective even for adversaries with access to large bonnets
2. The protocol should not have any significant impact on usability. For example: for legitimate users, any additional steps besides entering login credentials should be minimal. Increasing the security of the protocol must have minimal effect in decreasing the login usability.
3. The protocol should be easy to deploy and scalable, requiring minimum computational resources in terms of memory, processing time, and disk space.

System Architecture

This architecture have two entity used

1) User and 2) Web Server.

The web server will avoid online AI attacks using CAPTCHA mechanism; a new CAPTCHA mechanism will improve one step ahead for existing CAPTCHA mechanism. User successfully given user name and password that time will login to web server but user enter username and password multi time to give Captcha process, the use salve all captcha process and then access the web server. The PGRP protocol resistance for un known machine login over internet.

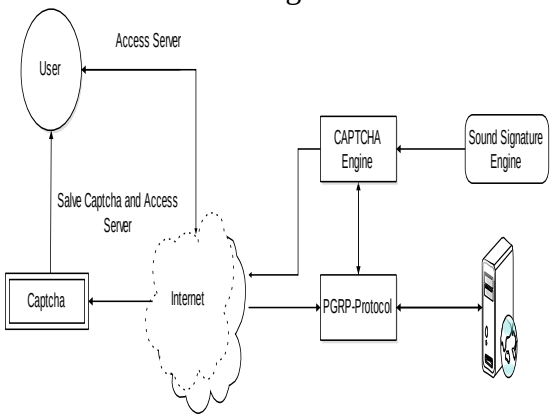

Figure5.Proposed System Architecture

VI. 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 introducesa 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-force attacks, 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 Animal Grid and Click Text easier to use than Pass Points and a combination of text password and Captcha. Both Animal Grid and Click Text had better password memo ability than the conventional text passwords. On the other hand, the usability of CaRP can be further improved by using images of different levels of difficulty based on the login history of the user and the machine used to log in. The optimal tradeoffs between security and usability remains an open question for CaRP, and further studies are needed to refine CaRP for actual deployments.

VII. FUTURE WORK

This project will implement for some extra security in AI problem, to Avoid anti fishing attack to use of mutual authentication protocol using hash generating function RIPEMD-160 which is RACE Integrity Primitives Evaluation Message Digest (RIPEMD-160), It is an improved version of RIPEMD, which in turn was based upon the design principles used in MD5, and is similar in performance to the more popular SHA- 1.

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.
[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 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/

