International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-3, Issue-2, March 2015

A New Security Primitive Based on Hard AI Problems and Efficient User Authentication using Captcha and Graphical Passwords

Miss. Bhagyashri A. Banarase , Prof. M. A. Kalyankar

***Abstract*—In this paper,I present a new security primitive based on hard AI (Artificial Intelligence) problems, namely, a novel family of graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP) [1].CaRP is a combination of both a captcha and a graphical password scheme [3].With the hybrid use of captcha and graphical password one can addresses a number of security problems such as relay attacks, online guessing attacks and also shoulder surfing attacks[4].a new security primitive based on hard AI problems, namely, a novel family of graphical password systems integrating captcha technology, which is called 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 CaRpare captcha challenges [7].The CaRP scheme is enhanced with more attack handling mechanisms that improves the level of security in online application system and also provides better authentication [6].**

***Index Terms*— AI, captaha, CaRP, Graphical password, User Authentication.**

I. INTRODUCTION

A Fundamental task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable [1]. The most common computer authentication method is for a user to submit a user name and text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also be easily guessed or broken [2].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 [1].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[3].

Manuscript received March 25, 2015.

Bhagyashri A. Banarase, computer science & engineering, sant gadge baba univercity, Amravati, India, Mobile No.8149609307,

Prof. Meghali A. kalyankar, computer science & engineering, sant gadge baba univercity, Amravati, India, Mobile No.8007092220,

II. RELATED WORK

A. *Graphical password*

Graphical passwords can be largely classified into three categories: recognition-based, cued-recall, or recall-based. [1]. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and, therefore, more secure[7] 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 advantages, there is an increasing interest in graphical password [3].

B. *captcha*

A captcha is a program that can generate and grade tests that: most humans can pass, but current computer programs cannot pass. Such a program can be used to differentiate humans from computers [3]. 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) [1].Text captha which relies on character recognition and Image recognition captcha which deals with the recognition of non-character objects. It is used to prevent sensitive user inputs on an entrusted client which protects the communication channel between the user and web server from key loggers [4].

C. *Captcha in Authentication*

It was introduced in 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[5].The CbPA-protocol in 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 [1]. An improved CbPA-protocol is proposed in 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 [5].

III. CAPTCHA AS GRAPHICAL PASSWORD

A. *New Way to Thwart Guessing Attacks*

In a guessing attack, a password guess tested in an unsuccessful trial is determined wrong and excluded from subsequent trials. The number of undetermined password guesses decreases with more trials, leading to a better chance of finding the password [1]. To counter guessing attacks, traditional approaches in designing graphical passwords aim at increasing the effective password space to make passwords harder to guess and thus require more trials. No matter how secure a graphical password scheme is, the password can always be found by a brute force attack [5].

The capability gap between humans and machines can be exploited to generate images so that they are computationally independent yet retain invariants that only humans can identify, and thus use as passwords. The invariants among images must be intractable to machines to thwart automatic guessing attacks. This requirement is the same as that of an ideal captcha leading to creation of CaRP, a new family of graphical passwords robust to online guessing attacks [1].

B. *Converting Captcha to CaRP*

In principle, any visual Captcha scheme relying on recognizing two or more predefined types of objects can be converted to a CaRP. All text Captcha schemes and most IRCs meet this requirement. Those IRCs that rely on recognizing a single predefined type of objects can also be converted to CaRPs in general by adding more types of objects. In practice, conversion of a specific Captcha scheme to a CaRP scheme typically requires a case by case study, in order to ensure both security and usability. CaRPs built on top of text and image-recognition Captcha schemes [1]. These IRCs cannot be converted into CaRP since a set of pre-defined object types is essential for constructing a password [5].

C. *User Authentication with CaRP Schemes*

Graphical password have been proposed as a possible alternative to text based, motivated particularly by the fact that humans can remember pictures better than text. [2].

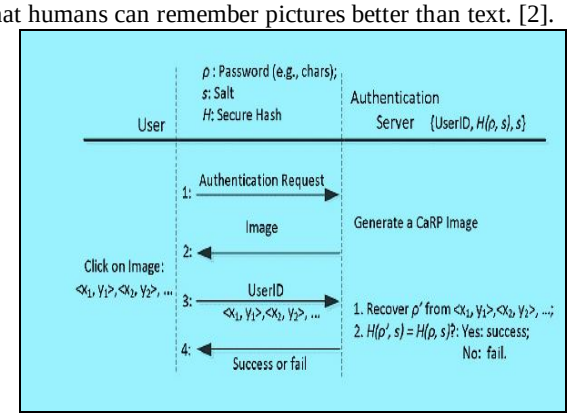

Fig 1: Flowchart of basic CaRP authentication.

Like other graphical passwords, we assume that CaRP schemes are used with additional protection such as secure channels between clients and the authentication server through Transport Layer Security (TLS) [5]. A typical way to apply CaRP schemes in explained in Flowchart, The authentication server AS stores a salt s and a hash value H (p,s) for each user ID, where is the password of the account and Not stored. A CaRP password is a sequence of visual object IDs or clickable-points of visual objects that the user selects [7].

Upon receiving a login request, AS generates a CaRP image, records the locations of the objects in the image, and sends the image to the user to click her password. The coordinates of the clicked points are recorded and sent to AS along with the user ID [5]. AS maps the received coordinates onto the CaRP image, and recovers a sequence of visual object IDs or clickable points of visual objects, that the user clicked on the image. Then AS retrieves salt s of the account, calculates the hash value of with the salt, and compares the result with the hash value stored for the account. Authentication succeeds only if the two hash values match [7]. To recover a password successfully, each user-clicked point must belong to a single object or a clickable-point of an object. [1].

IV. RECOGNIZATION 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 [1].

A. clickText

ClickText is a CaRP scheme built on top of text Captcha. Unlike normal text Captch as, a CaRP image should contain the entire alphabet to allow a user to for many allowed password. In ClickText images, characters can be arranged randomly on 2D space this is another major difference from traditional text Captch as in which characters are typically ordered from left to right. Using ordinary text Captcha is not suitable in this context, as it is hard to arrange the entire characters one dimensionally in a reasonably small space. Also, there is no order among characters in a CaRP image whereas the order is needed for characters in a normal Captcha image so that users can type them in. Therefore, we propose a new problem, 2D text segmentation, as the underlying hard AI problem for ClickText[6].

Fig. 2.A ClickText image with 33 characters

In ClickText 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. Fig. 2 shows a ClickText 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", and then "7" for Password ρ = "AB#9CD87"[1].

B.ClikAnimal

Fig. 4. Captcha Zoo with horses circled red.

ClickAnimal 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 [1]. 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 [5].

Some animals may be overlapped by other animals in the image, but their core parts are not overlapped in order for humans to identify each of them. 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[3].

C.AnimalGrid

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 [1]. CaRP should have a sufficiently-large effective password space to resist human guessing attacks. Animal Grid'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 [5]. DAS 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. AnimalGridis 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 grid-cell at the authentication server side when the correct grid is used [1].To enter a password, a ClickAnimal image is displayed first. After an animal is selected, an image of

n × n grid appears, with the grid-cell size equaling the bounding rectangle of the selected animal. Each grid-cell is labeled to help users identify [5].Fig. 4 shows a 6 × 6 grid when the red turkey in the left image of Fig. 4 was selected. A user can select zero to multiple grid-cells matching her password. 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 [6].

Fig. 4. A ClickAnimal image (left) and 6 × 6 grid (right) determined by red turkey's bounding rectangle.

V. RECOGNITION –RECOL 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 [1]. 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 [5].

A. TextPoints

In TextPoints characters contain invariant points which offer 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. A password is a sequence of clickable points. A character can typically contribute multiple clickable points [4].

In TextPoints characters contain invariant points which offer 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. A password is a sequence of clickable points. A character can typically contribute multiple clickable points [2]

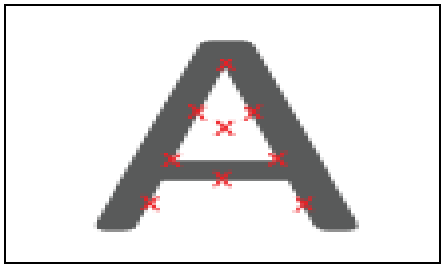

Fig.5. some invariant points (red crosses) of "A".

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[1].

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 [5]. A character can typically contribute multiple clickable points. Therefore TextPoints has a much larger password space than ClickText. For challenge-response authentication protocol, a response is sent to the authentication server [4].

B. TextPoints4CR

TextPoints can be modified to fit challenge-response authentication. This modification 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[4].TextPoints can be modified to fit challenge response authentication. This variation is called TextPoints for Challenge-Response or TextPoints4CR [2]. 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 in TextPoints4CR should generate the same sequence of discredited 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 [1].

VI. CONCLUSION

Captcha as a graphical password introduces new family of graphical password which acts as a firewall for online guessing attacks. A password of CaRP can only be recognized through brute force attack[1].It is a fundamental method in computer security to create cryptographic primitives based on hard mathematical problems that are computationally intractable Using hard AI problems for security, initially proposed in, is an exciting new paradigm [6]. This Paper Reviews Various Types of Captchas Such AsClicTtext, ClickAnimal, AnimalGrid, TextPoints and TextPoints4cr.Further the usability of CaRP image is improved through images of different level of hardness based on log in history of the user and the machine used for the log in purpose [4].

.

REFERENCES

[1] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, And Ning Xu," Captcha As Graphical Passwords - A New Security Primitive Based On Hard AI Problems, "IEEE Transactions On Information Forensics And Security, Vol. 9, No. 6, June 2014 891.

[2]Magniya Davis , Divya R ,Vince Paul &Sankaranarayanan P N ,"CAPCHA as Graphical Password," Magniya Davis et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, 148-151 ISSN : 0475-9646.

[3]Jayshree Ghorpade , Shamika Mukane , Devika Patil , Dhanashree Poal , & Ritesh Prasad , "Novel Method for Graphical Passwords using CAPTCHA," International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-4 Issue-5, November 2014 ,77 Published By: Blue Eyes Intelligence Engineering& Sciences Publication Pvt. Ltd.

[4]Nayan Gawande Computer Engineering, J. S. P. M, Tathawade, Pune, India – 411033, "Merging CAPTCHA and Graphical Password on NP Hard Problems in AI: New Security Enhancing Technique," International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Impact Factor (2012): 3.358.

[5]ValusaniShrenika&Mr.D.UmaVishweshwar," Captcha as Graphical Passwords Security Primitive Based On Hard Ai Problems," International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 National Conference on Developments, Advances & Trends in Engineering Sciences (NCDATES- 09th & 10th January 2015) CMR Engineering College .

[6] Bin B. Zhu and Jeff Yan, "Towards New Security Primitives Based on Hard AI Problems,"
B. Christianson et al. (Eds.): Security Protocols 2013, LNCS 8263, pp. 3–10, 2013.

[7]Ganesh B. Gadekar& Prof. N. G. Pardeshi," Providing More Security Using Graphical Password- CaRP," ISSN (Online): 2347-1697 International Journal of Informative & Futuristic Research (IJIFR) Volume 2, Issue 3, November 2014 15th Edition.

Miss. Bhagyashri A. Banarase, computer science & engineering, sant gadge baba univercity, Amravati, India, Mobile No.8149609307,

Prof. Meghali A. kalyankar, computer science & engineering, sant gadge baba univercity, Amravati, India, Mobile No.8007092220,