A Survey On CAPTCHA As Graphical Passwords Overcomed By Virtual Passwords Schemes

S.Karthika[#1],P.Tharcis [*2]

[#] PG Scholar, Department of Computer Science and Engineering, Christian College of Engineering and Technology, Dindigul, Tamilnadu - 624619, India.

[1]Karthivaishu22@gmail.com

* Assistant Professor, Department of Electronics and Communication Engineering, Christian College of Engineering and Technology, Dindigul, Tamilnadu - 624619, India.

[2]ptharcis@gmail.com

***Abstract*- Passwords which are graphical are believed to be more secure than the textual passwords.Here the authentications are boring and complex for users. Moreover,the existing graphical passwords scheme are vulnerable to shoulders-shurfing and spyware.Even most of these alternate schemes have their own merits and demerits. Forinstance,cued-recall graphical passwords schemes are vulnerable to shoulder-surfing and intersection analysis attack is not prevented.So that, CAPTCHA as graphical passwords has been overcome by a virtual password scheme (deal with secret little function method and a code book technique) that acts as a proposal in this paper. And here by using virtual password scheme the passwords are in a differentiated manner including usability, security and Implementation considerations. Furthermore, a Hard AI problem supports the security primitives.**

***Index Terms*- CaRP, click-Text, authentication, AnimalGrid, virtual password scheme.**

I. INTRODUCTION

An alternative proposal to alphanumeric passwords is graphical passwords with their advantages of usability and security. Figure 1 shows the normal login process that s used by the authenticated users. Here,this proposal deals with a large number of the graphical password schemes.They can be classified into two 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 [1]with an increasing number of free services on the internetand find a pronounced need to protect these services from abuse.CAPTCHA is now a standard internet security technique to protect online E-mail and other services from being abused by bots. Although,there is a possibilities of hacking that may be done by particular attacks.

Figure 2 shows the login activity with CAPTCHA as a security. Now we introduce secret little function method in CaRP which is resistant from Automatic online guessing attacks, Human guessing attacks, shoulder surfing attacks, Relay attacks.

An existing CaRP approaches method using in text click and animal click technical. The method used is memorizing and clicking password scheme.The proposed system using secret little function method. A one-time password does not use a static password and therefore can prevent relay attacks. The password randomly generated on mathematical algorithm.CAPTCHA is used to protect sensitive user inputs on an untrusted client

Fig 1.Login process

.II.PREVIOUS CaRP SCHEMES

In CaRP (CAPTCHA as gRaphical Passwords), a new image is generated for every login attempt, even for the same user. CaRP uses an alphabet of visual objects (e.g., alphanumerical characters, similar animals) to generate a CaRP image, which is also a CAPTCHA challenge. A major difference between CaRP images and CAPTCHA images is that all the visual objects in the alphabet should appear in a CaRP image to allow a user to input any password but not necessarily in a CAPTCHA image. Many CAPTCHA schemes can be converted to CaRP schemes, as described in the next subsection.

CaRP schemes are clicked-based graphical passwords. According to the memory tasks in memorizing and entering a password, CaRP schemes can be classified into two categories: recognition and a new category, recognition-recall, which requires recognizing an image and using the recognized objects as cues to enter a password. Recognition-recall combines the tasks of both recognition and cued-recall, and retains both the recognition-based advantage of being easy for human memory and the cued-recall advantage of a large password space.

Fig 2.CAPTCHA as a password security.

A. A recognition-based scheme

This scheme requires identifying among decoys the visual objects belonging to a password portfolio. A typical scheme is Passfaces[2] 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. We present two recognition-based CaRP schemes and a variation next.

1) ClickText

ClickText is a recognition-based CaRP scheme built on top of text CAPTCHA. Its alphabet comprises characters without any visually-confusing characters. A ClickText password is a sequence of characters in the alphabet, e.g., ρ ="AB#9CD87", which is similar to a text password. A ClickText image is

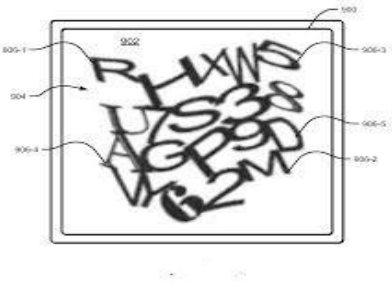

Fig 3.A ClickText images

generated by the underlying CAPTCHA engine as if a CAPTCHA image were generated except that all the alphabet characters should appear in the image. During generation, each character's location is tracked to produce ground truth for the location of the character in the generated image. The authentication server relies on the ground truth to identify the characters corresponding to user-clicked points.

2) ClickAnimal

ClickAnimal is a recognition-based CaRP scheme built on top of CAPTCHA Zoo [8], with an alphabet of similar animals such as dog, horse, pig, etc. CAPTCHA Zoo [8] is a CAPTCHA scheme which uses 3D models of horse and dog to generate 2D animals with different textures, colors, lightings and poses, and arranges them on a cluttered background. A user clicks all the horses in a challenge image to pass the test.

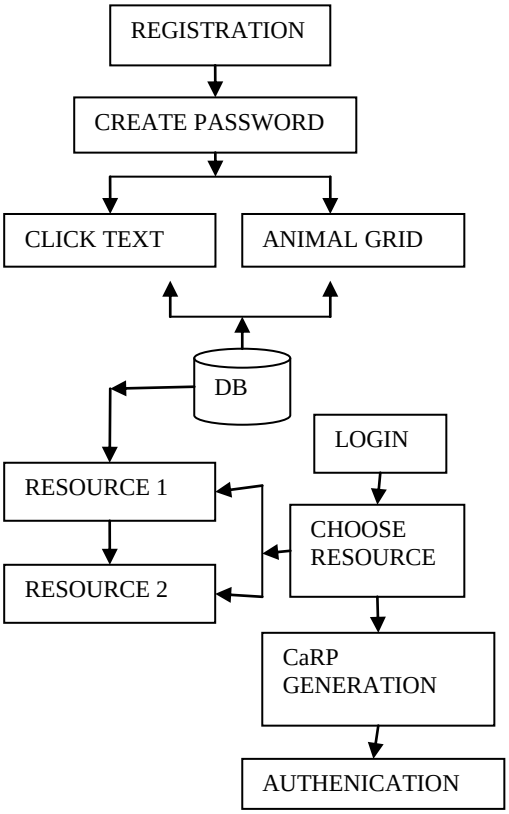

Figure 4. Animal grid and click text processing method

3) AnimalGrid

AnimalGrid is a combination of ClickAnimal and (CAS) Click-A-Secret. 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. When a ClickAnimal image appears, the user clicks the animal on the image that matches the first animal in her password. The coordinates of user-clicked points on the grid image (the original one before scaling if the grid image is scaled) are recorded. The above process is repeated until the user has finished entering her password. Figure 4 shows about the processing activities of the authentication process with the choosing of resources.
CAPTCHA is applied touch screen method so suddenly if some fault then user could not access the login process. Here, shoulder-surfing attacks are possible.

B. A recall-based scheme

In recognition-recall CaRP, a password is a sequence of some invariant points of objects requires a user to regenerate the same interaction result without cueing.
Draw-A-Secret (DAS) [3] was the first recall-based scheme proposed. A user draws her password on a 2D grid. The system encodes the sequence of grid cells along the drawing path as a userdrawn password. Pass-Go [4] improves DAS's usability by encoding the grid intersection points rather than the grid cells. BDAS [7] adds background images to DAS to encourage users to create more complex passwords.

1) TextPoints

Characters contain 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. 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.

Fig 5.Some invariant points of "A"

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.

2) TextPoints4CR

The coordinates of user-clicked points are sent directly to the authentication server during authentication. For more complex protocols, say a challenge-response authentication protocol, a response is sent to the authentication server instead. TextPoints can be modified to fit challenge-response authentication. This variation is called TextPoints for Challenge-Response or TextPoints4CR.

Image Generation:To generate a TextPoints4CR image, the same procedure to generate a TextPoints image is applied. Then the following procedure is applied to make every clickable point at least τ distance from the edges of the grid-cell it lies in. All the clickable points, denoted as set F, are located on the image. For every point in F, we calculate its distance along x-axis or y-axis to the center of the grid-cell it lies in. A point is said to be an internal point if the distance is less than $0.5\mu-\tau$ along both directions; otherwise a boundary point. For each boundary point in F, a nearby internal point in the same grid-cell is selected. The selected point is called a target point of the boundary point. After processing all the points in F, we obtain a new set F comprising internal points; these are either internal clickable points or target points of boundary clickable points.

Authentication:In entering a password, a user-clicked point is replaced by the grid-cell it lies in. If click errors are within τ , each user-clicked point falls into the same grid-cell as the original password point. Therefore the sequence of grid-cells generated from user-clicked points is identical to the one that the authentication server generates from the stored password of the account. This sequence is used as if the shared secret between the two parties in a challenge-response authentication protocol.

Moreover, the stored passwords must be protected from inside attacks and attackers.This did not introduce the notion of CARP or explore its rich properties and the design space of a variety of CARP instantiations.

III. POSSIBLE ATTACKS TO CRACK PASSWORDS

A. Online Guessing Attacks

Online guessing attacks on password-based systems are inevitable and commonly observed against web applications. The purpose is to prevent the online guessing attacks namely brute force and dictionary attacks which aim at gaining an unauthorized access to the valid user's data. Figure 6 shows the online guessing attacks that are happened in the CAPTCHA systems.

Brute force attack is the method of trying every possible code, combination, or password until you find the correct one. This is sometime time consuming if the password involves some hash method.

Dictionary attack is the method to guess passwords which is achieved using common list of words to identify the user's password. A dictionary attack uses a targeted technique of successively trying all the words in an ex-haustive list called a dictionary that is from a pre-arranged list of values.

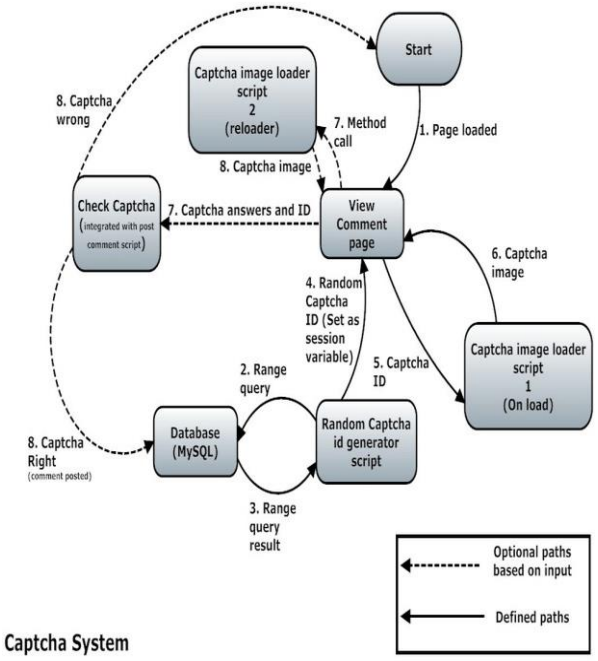

Fig 6.Online guessing attacks in CAPTCHA system.

B. Human Guessing Attacks

In human guessing attacks, humans are used to enter passwords in the trial and error process. Humans are much slower than computers in mounting guessing attacks. For 8-character passwords, the theoretical password space is 338 ≈ 240 for ClickText with an alphabet of 33 characters, 108 ≈ 226 for ClickAnimal with an alphabet of 10 animals, and 10 × 467 ≈ 242 for AnimalGrid with the setting as ClickAnimal plus 6×6 grids. If we assume that 1000 people are employed to work 8 hours per day without any stop in a human guessing attack, and that each person takes 30 seconds to finish one trial. It would take them on average 0.5 · 338 ·30/(3600 · 8 · 1000 · 365) ≈ 2007 years to break a ClickText password, 0.5 · 108 · 30/(3600 · 8 · 1000) ≈ 52 days to break a ClickAnimal password, or 0.5 · 10 · 467 · 30/(3600 · 8 ·1000 · 365) ≈ 6219 years to break an AnimalGrid password. Human guessing attacks on TextPoints require a much longer time than those on ClickText since TextPoints has a much larger password space. Just like any password scheme, a longitudinal evaluation is needed to establish the effective password space for each CaRP instantiation.

C. Shoulder-surfing attacks

Shoulder-surfing is an attack on password authentication that has traditionally been hard to defeat. It can be done remotely using binoculars and cameras, using keyboard acoustics [11], or electromagnetic emanations from displays [12]. Access to the user's password simply by observing the user while he or she is entering a password undermines all the effort put in to encrypting passwords and protocols for authenticating the user securely.

To some extent, the human actions when inputting the password are the weakest link in the chain. Shoulder-surfing(Figure 8) is of particular concern in recognition-based systems when an attacker can record or observe the images selected by users during login. This is especially problematic for this category of schemes because there are relatively few images (indeed, the theoretical password space is small) and the images selected by users are large discrete units that may be more easily identifiable.

Consequently, many recognition-based schemes have specific mechanisms to address this threat. or example, in many systems users perform some action based on the location of their portfolio images within a panel of images, without directly selecting their images. Varying the presented location of portfolio images, as determined by the system, creates a form of challenge-response system.

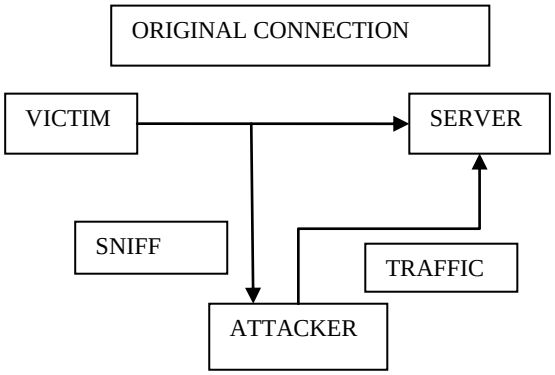

Fig 8.Shoulder-surfing attacks

Shoulder-surfing is a targeted attack exacerbated by the visual aspect of graphical passwords.

D. Relay Attacks

A Relay attack is a type of hacking technique related to man-in-the-middle and replay attacks, in which an attacker relays verbatim a message from the sender to a valid receiver of the message. The sender may or may not be aware of even sending the message to the attacker; if the sender is aware, it is likely under the impression that the attacker is the intended receiver of the message.

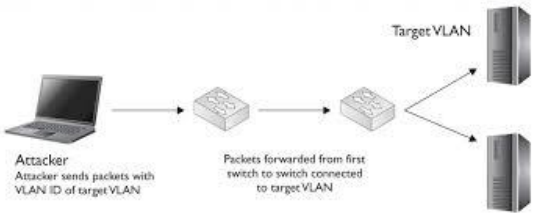

Fig 9.Relay attacks

Relay attacks(Figure 9) may be executed in several ways. CAPTCHA challenges can be relayed to a high-volume Website hacked or controlled by adversaries to have human surfers solve the challenges in order to continue surfing the Website, or relayed to sweatshops

where humans are hired to solve CAPTCHA challenges for small payments. Is CaRP vulnerable to relay attacks? We make the same assumption as Van Oorschot and Stubblebine[13] in discussing CbPA-protocol's robustness to relay attacks: a person will not deliberately participate in relay attacks unless paid for the task. The task to perform and the image used in CaRP are very different from those used to solve a CAPTCHA challenge. This noticeable difference makes it hard for a person to mistakenly help test a password guess by attempting to solve a CAPTCHA challenge.

In the above schemes,there are many drawbacks in which these attacks can be prevented using the proposal systems in which to overcome that this paper introduces a new idea using virtual password scheme.

IV. FUTURE ENHANCEMENTS AND IMPLEMENTATIONS

Based on our evaluation,the proposed system uses the little function method and in which the virtual password is a dynamic password that is generated differently each time from a virtual password scheme and then submitted to the server for authentication.A one-time password doesnot use a static password and therefore can prevent relay attacks.The password randomly generated on mathematical algorithm.Moreover,it s a software oriented approach.This ensures ease of computation and even security is high.Furthermore, our implementations for securing the passwords in a textual way is based upon virtual password scheme which has certain functions like default, user specified function, user specified programs instead of text based CAPTCHA passwords.

The future idea is based upon the Codebooks for Protecting Users from Password Theft in which the method to generate the logfile and then create a random number.To assume that our server has sufficient computing power to run a cryptographically secure random number generator.More accurately,this requirement is necessary to protect one whole system. Overall, based on our evaluation a new security primitive is introduced.

V. CONCLUSION

The main purpose of authentication schemes is allowing system access only by legitimate users.Although many specified techniques are there is a chance of many hacking possibilities.Based on our evaluation,these can be avoided and passwords can be maintained in a way that is secured by dynamic activities.

In addition to the importance of evaluation, code books concepts are implemented in a secure manner from password thefts.After examining each challenge and its responses,this paper concludes that the password can also be secured in a clearway using virtual password schemes.

VI. 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]. HP TippingPoint DVLabs, Vienna, Austria. (2010). Top Cyber Security Risks Report, SANS Institute and Qualys Research Labs [Online]. Available: http://dvlabs.tippingpoint.com/toprisks2010

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

[7]. P. Dunphy and J. Yan, "Do background images improve 'Draw a Secret' graphical passwords," in Proc. ACM CCS, 2007, pp. 1–12.

[8]. 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.

[9]. J. Jayavasanthi Mabel1, Mr. C.Balakrishnan2, "RESISTING PASSWORD BASED SYSTEMS FROM ONLINE GUESSING ATTACKS" International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013).

[10]. J. Bonneau, "The science of guessing: Analyzing an anonymized corpus of 70 million passwords," in Proc. IEEE Symp. Security Privacy, Jun. 2012, pp. 20–25.

[11]. Zhuang, L., F. Zhou, and J. D. Tygar. Keyboard Acoustic Emanations Revisited. In Proceedings of Computer and Communications Security (CCS). Alexandria, Virgina, USA: ACM Press. pp. 373-82, 2005.

[12]. Kuhn, M. G., Electromagnetic Eavesdropping Risks of Flat- Panel Displays, in 4th Workshop on Privacy Enhancing Technologies, LNCS. Springer-Verlag: Berlin / Heidelberg. pp. 23–25, 2004.

[13]. 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.

