ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

DOGGY – a Graphical Security Technique to prevent Online Guessing Attacks

S.Sachin Shriram[1], Dr.K.P.Kaliyamurthie[2]

Student, Dept of C.S.E, Bharath University, Chennai, Tamil Nadu, India[1].

Head of the Dept, Dept of C.S.E, Bharath University, Chennai, Tamil Nadu, India[2].

ABSTRACT: New Security Techniques emerge everyday to ensure the safety of a system. The Graphical Password Technique called CaRP(Captcha as gRaphical Passwords) is built on CAPTCHA Technology. This paper proposes DOGGY (Distinct Organized Genius Graphical keY) which is built on multiple layers of CaRP which secures the system from Online Guessing Attacks. The sophistication of DOGGY helps users to secure their systems through a wide layered security which is complex to crack, providing a stronger password choice. DOGGY offers optimum security and can be used for a wide range of applications that require rigid security.

KEYWORDS: CaRP, guessing attack, graphical password, security, Captcha, DOGGY, integrity

I. INTRODUCTION

The need for security is growing and every security shield is broken and prohibited access of data takes place in the world. Online Guessing Attacks are one such way to bypass the system through guessing common passwords and combinations. This proved to be a challenge to the tradional text passwords since they could be deciphered if some time and effort was put into cracking them.

Hence newer password techniques started emerging such as CaRP, Picture Passwords, etc. Captcha as gRaphical Passwords known as CaRP is a technique based on Completely Automated Public Turing tests to tell Computers and Humans Apart i.e, CAPTCHA. But in time, even these techniques start to succumb to attacks since they are single layered. These systems performed independently and newer levels were not added to them.

Improvising on CaRP, we build DOGGY a greater system of security and protection that has multiple layers. Doggy stands for Distinct Organized Genius Graphical keY. The layers are a combination of different graphical password techniques which follow separate routines to clear. Since there is a distinct routine to clear each level, it has a greater notion of security thus securing in a way that is better than its predecessors.This is the first step taken towards building a graphical password system with multiple layers thereby enhancing security.

II. RELATED WORK

A. Draw a Secret

When only text passwords were present, a new technique was required to stand out and protect data in a way that is different. The idea of graphical passwords materialised as it made use of Graphical Input such as a pattern that could be drawn. This technique is the first proposition to bring Graphical Passwords into existence. In this technique, the password is a simple pattern drawn on a grid. The technique is independent of alphabet knowledge, hence making this easily accessible for all users irrespective of language. Users are freed from having to remember any kind of alphanumeric string.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

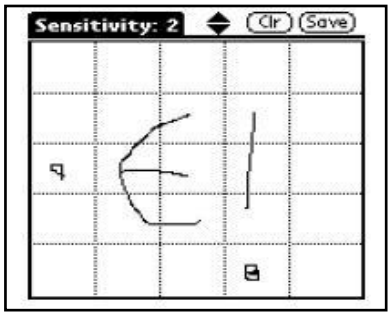

Fig. 1. Draw a Secret

Exploiting the use of graphical input, users were asked to draw their pattern onto an area using the mouse. This pattern would then be saved for that user and then used for further logins. This technique called Draw a Secret enabled users to get out of the tradition that is text passwords. While this scheme is outdated it is still seen in PDA applications for drawing signatures in forms and receipts.

B. Pass-Go

Draw a Secret scheme leaded the way in the evolution of newer graphical passwords. Even though the DAS scheme was a success, it was time consuming and drawing patterns did not seem the way to secure passwords since it required artistic skills with the mouse. The Pass-Go scheme followed a system that was easier than DAS and at the same time better.

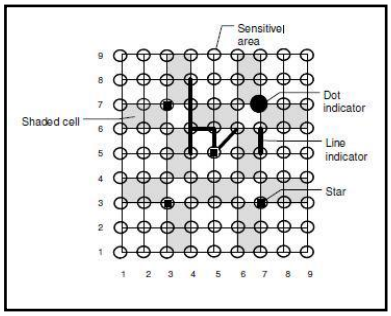

Fig. 2. Pass Go

As the name implies, Pass-Go is a grid-based scheme. However, different from DAS, Pass-Go requires a user to select (or touch) intersections, rather than cells, to input a password. Eventually, the coordinates system redirects to a matrix of intersections, rather than cells as in DAS.Pass-Go's interface has a grid with intersections. Users select the intersections in a sequence and this is their password. The password space is large and hence gives room for many password combinations. The major use of this scheme was seen in extended devices other than PDA.

C. Passpoints

Pass-Points not unlike Pass-Go, was a development of the graphical password system after Draw a Secret. Instead of selecting intersections, Pass-Points asked users to select points of a picture and this was easier to comprehend than grids in Pass-Go.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Fig. 3. Passpoints

In the password creation phase the user was given instructions on the screen to create a password. Graphical password users had to select and enter five distinct points on the picture with no point within the tolerance around any other chosen point. Considering the above example, the picture of a crowd is given and several points are clicked in succession. This sequence is the password of the user and used for further logins. Users were able to create valid passwords with fewer difficulties than creating passwords composed of alpha-numeric-special characters.

D. Captcha

Unlike other systems the CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) system was created to prevent redundant or spam creation of accounts and filling of surveys. This system was introduced as a first when none existed for its purpose.

Fig. 4. Text Captcha

CAPTCHA is basically a test of imitations.CAPTCHA's turing test involved distorted letters that could be perceived by the creative human brain but not by bots that are used to read text. The most common form of CAPTCHA is an image of several distorted letters. The first among this was the Text CAPTCHA that had letters warped and distorted and only by entering the text could the survey be submitted or the email account be created. The CAPTCHA test helps identify which users are real human beings and which ones are computer programs. A CAPTCHA form can help prevent programmers from taking advantage of the polling system. Some CAPTCHAs rely on pattern recognition and extrapolation. A CAPTCHA might include a series of shapes and ask the user which shape among several choices would logically come next.

E. Cued ClickPoints

The Cued Click Points (CCP) scheme is a proposed alternative to Pass Points. In Cued ClickPoints, users click one point of each of the 5 images rather than on five points on one image.The Pass-Points graphical scheme used a sequence in the same image and that seemed easier to decipher since hot-spots could be identified. Due to this reason, Cued Click Points were introduced which followed a sequence of clicks in a sequence of images.

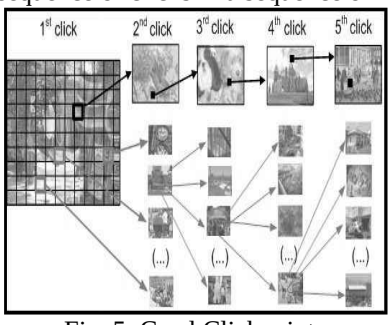

Fig. 5. Cued Clickpoints

First the user would click a point in an image and if it is correct, proceeds to the next image until 5 clicks. Once the sequence is correct the user is granted access. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their newest click point. Additionally it makes attacks on hotspot identification analysis more complex. A wrong click results an incorrect sequence, with consequent authentication error only after the final click.

F. Persuasive Cued ClickPoints

Poorly chosen passwords lead to emergence of hotspots. Even though Cued Click Points were built to solve this issue, even that had several hotspots. It allows attackers to guess where users are more likely to choose clickpoints. Hence Persuasion was introduced in Cued Click Points and named Persuasive Cued Click Points. The primary goal of PCCP was to increase the effective password space by guiding users to select more random passwords.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Fig. 6. Persuasive Cued Clickpoints

Persuasion guides users to select stronger password choice thus influencing stronger click passwords and discouraging hotspots. An authentication system which applies Persuasive Technology should guide and encourage users to select stronger passwords, but should not encourage system generated keys. For effectiveness, the users must follow the persuasive elements and the resulting passwords must be memorable.

G. Cortchas

When CAPTCHA was introduced only Text CAPTCHAs prevailed. To introduce a graphical presence of images, CORTCHA (Context-based Object Recognition to Tell Computers and Humans Apart) was introduced. CORTCHA used context based object recognition in humans as the concept in creating the system.

Fig. 7. Cortcha

A Cortcha challenge displays an inpainted image along with candidate objects. A user selects a candidate object, and drags it to move around or drop to a position of the inpainted image. The buffer region is cropped and then filled by an image smoothing methodTaking the above example, flowers would be picked out of the plant and the users would be asked to place them at the right place. This means infinite possibilities could be generated to create challenges. This re-arrange method was a step forward than what was present. Effectively, a composite image is created by combining the inpainted image and the candidate object on the spot.

H. Asirra Captcha

While CORTCHA used Context Recognition, it seemed that it was a tedious process to solve. So another easy and cute method of CAPTCHA was created called the Asirra CAPTCHA. It used Cats and Dogs in the identification test and differed from other basic image recognition CAPTCHAs.

Fig. 8. Asirra Captcha

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Asirra surmounts the image-generation problem in a novel way: by forming a partnership with Petfinder.com , the world's largest web site devoted to finding homes for homeless pets. Asirra generates challenges by displaying 12 images from a database of over three million photographs that have been manually classified as cats or dogs. .Asirra used 12 photos that had both cats and dogs. The users were asked to identify only the Cats from the set. This system is based on exploting Interest Aligned Categorization. The images used on the system were supplied by the website.

III. EXISTING METHODS

A. ClickText

Distorted alphanumerals and special characters are provided from which the user can select a sequence of characters to be their password and used for further logins. It is basically an improvement of the text captcha as a password.

Fig. 9. ClickText

B. ClickAnimal

Animal figurines are provided in different colours and sizes for distinct identification from which the user can select a sequence and save as their password. This is later used for further authentication purposes.

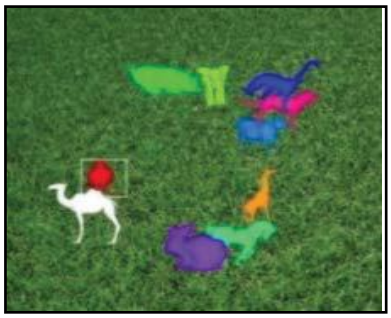

Fig. 10. ClickAnimal

C. CaptchaZoo

This system originally not a password technique but identification scheme to select similar coloured animals in a picture. Once the user completes the test correctly he is granted access to the files or the following page.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Fig. 11. CaptchaZoo

D. Disadvantages of these systems

While all the above systems provided a unique solution from text passwords, they lack the ability to protect the system after an attack has breached the system. Therefore here Doggy comes into place and its multiple layers help in this purpose by creating complexity for attackers or hackers who try to access the system unauthorized.

IV.DOGGY ARCHITECTURE

The Doggy system architecture has three layers, each of which has a unique method of password verification that enables every layer to distinct itself from the other.

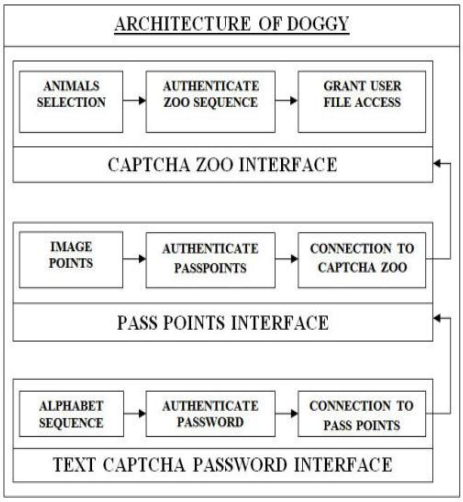

Fig. 12. DOGGY Architecture

The process and function of each layer is discussed below.

A. Text CAPTCHA Password

TextCAPTCHA Password is a text recognition CaRP scheme which has distorted alphabets from which the user gets to chose their password. Alphabets are clicked in succession and saved as the password once the sequence is complete. The letters provided might me alphabets, numbers or special characters or a variety of all.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

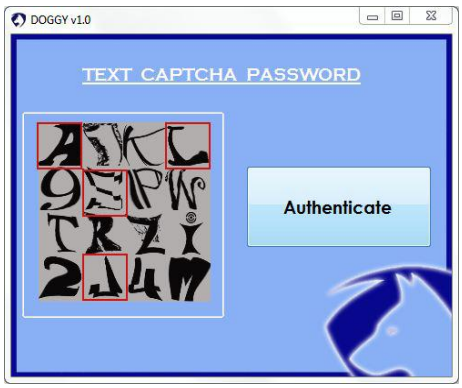

Fig. 13. Text Captcha Password Interface

The distortion provided in these images confuse bots and computers whereas humans can perceive it. This enables the security against intrusion by bots. Once this layer is cleared the user is directed to the next layer.

B. PassPoints

A picture of reality as a workplace or a crowd is provided and the users are asked to select a sequence to be saved as their password. The sequence that the user can select are segments of the image say a coordinates which are not perceived by bots since it is just an image.

Fig. 14. PassPoints Interface

Therefore requirement of man power is needed to crack the system which takes a lot of effort and resource therefore less prone to attacks. During further logins, the users have to get this sequence correct after which they are granted access to the next layer of the system.

C. CaptchaZoo

The original CaptchaZoo system was for a security primitive where users were asked to select similar coloured animals to pass through the turing test of whether they are human or computer. But in this system, it is used as a Password primitive. Animated faces of animals are provided and several of these faces could be selected as a sequence thereby saving the password.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Fig. 15. CaptchaZoo Interface

This sequence is repeated during each login and thereby authenticating oneself to the system. This is the final layer of the system and once cleared, the user is granted access to their files.

Fig. 16. Final Authentication Screen

D. Advantages of Doggy

The Multiple layers present in the system enable extra security to the user file integrity and hence ensuring safety. Since every layer of the system is unique, cracking the layer of its password requires a lot of man power and resource and hence is a tedious work. The need for improved security is established by the additional layers that provide a higher level of sophistication than its predecessors let it be the traditional text passwords or previous graphical password schemes.

V.CONCLUSION AND FUTURE ENHANCEMENTS

To sum up, Doggy is a new security primitive that relies on solving CAPTCHA as Graphical passwords. This system acts as both a Captcha and also as a password system. This is a development to the existing family of graphical passwords adopting new techniques to prevent online guessing attacks. The usability of Doggy is mainly for systems and files that require greater security against hackers.

Doggy is a step ahead in the paradigm of CaRP and it is a reasonable development over the existing systems and it hopes to inspire and aspire developers to create newer inventions and better systems in the future , for the growth of captcha and graphical passwords as a security measure.

Enhancements that can be made to the system are dependant on future technologies and innovations. As of now the system can be improved by adding real time password creation by users uploading their images at the moment and selecting their passwords instead of having pre defined images.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

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. (2012, Feb.).
2. 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.
3. H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," *Int. J. Netw. Security*, vol. 7, no. 2, pp. 273–292, 2008.
4. 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.
5. Adams, A., Sasse, M.A., 1999. Users are not the enemy. Communications of the ACM 42 (12), 41–46.
6. Bahrick, H.P., 1984. Semantic memory content in permastore: fifty years of memory for Spanish learned in school. Journal of Verbal Learning and Verbal Behavior 14, 1–24.
7. Biederman, I., Glass, A.L., Stacy, E.W., 1973. Searching for objects in real world scenes. Journal ofExperimental Psychology 97, 22–27.
8. irget, J.C., Hong, D., Memon, N., 2003. Robust discretization, with an application to graphicalpasswords. Cryptology ePrint Archive http://eprint.iacr.org/2003/168. Accessed January 17, 2005.
9. Blonder, G.E., 1996. Graphical passwords. United States Patent 5559961.
10. Boroditsky, M., 2002. Passlogix password schemes.
11. Bradley, M.M., Grenwald, M.K., Petry, M.C., Lang, P.J., 1992. Remembering pictures: pleasure and arousal in memory. Journal of Experimental Psychology 81 (2), 379–390.
12. Brostoff, S., Sasse, M.A., 2000. Are Passfaces more usable than passwords: a field trial investigation. In:McDonald, S., et al. (Eds.), People and Computers XIV—Usability or Else, Proceedings of HCI 2000. Springer, Berlin, pp. 405–424.
13. Brown, A.S., Bracken, E., Zoccoli, S., Douglas, K., 2004. Generating and remembering passwords. Applied Cognitive Psychology 18, 641–651.
14. L. von Ahn, M. Blum, N. Hopper, and J. Langford. CAPTCHA: Using hard AI problems for security. In Eurocrypt, LNCS, vol. 2656. May 2003, pp.294–311.
15. Greg Mori and Jitendra Malik. Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA. IEEE Conference on Computer Vision and Pattern Recognition, June 2003(1), pp.134-141.
16. M. Boldt, B. Carlsson, and A. Jacobsson. Exploring Spyware Effects, In Proceedings of the 8th Nordic Workshop on Secure IT Systems (NordSec04), Helsinki, Finland, 2004.