Novel Method for Graphical Passwords using CAPTCHA

Jayshree Ghorpade, Shamika Mukane, Devika Patil, Dhanashree Poal, Ritesh Prasad

Abstract-Cyber security is an important issue to tackle. Various user authentication methods are used for this purpose. It helps to avoid misuse or illegal use of highly sensitive data. Text and graphical passwords are mainly used for authentication purpose. But due to various flaws, they are not reliable for data security. Text passwords are insecure for reasons and graphical are more secured in comparison but are vulnerable to shoulder surfing attacks. Hence by using graphical password system and CAPTCHA technology a new security primitive is proposed. We call it as CAPTCHA as gRaphical Password (CaRP). CaRP is a combination of both a CAPTCHA and a graphical password scheme. In this paper we conduct a comprehensive survey of existing CaRP techniques namely ClickText, ClickAnimal and AnimalGrid. We discuss the strengths and limitations of each method and point out research direction in this area. We also try to answer "Are CaRP as secured as graphical passwords and text based passwords?" and "Is CARP protective to relay attack?"

Keywords:- CAPTCHA, CaRP, passwords, graphical, techniques.

I. INTRODUCTION

Security awareness is an important factor in an information security program. While organizations and institutes expand their use of advanced security technology and continuously train their security professionals, fraction of it is used to increase the security awareness among the normal users. As a result, today, organized cyber criminals are trying hard towards research and development of advanced hacking methods that can be used to steal money and secured information from the general public. Password authentication is one of the most common building blocks in implementing access control. Each user has a relatively short sequence of characters commonly referred to as a password. To gain access, providing right password is essential. Common attack for breaking password authenticated systems is dictionary attack [2]. Graphical password is an option for alphanumeric password as text password is slightly hard to remember text password. When any application is provided with user friendly authentication it becomes easy to break and use that application. Cloud security can also be given by alphanumeric password but thing matter is that use of alphanumeric is not that much of secure and easy to remember. Any individual examining the password can memorize it which may lead to its misuse.

Graphical password schemes are more reliable and more resilient to dictionary attacks than textual passwords, but more vulnerable to shoulder surfing attacks [3]. CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) is a program that generates and grades tests that are human solvable, but current computer programs do not have the ability to solve them. The robustness of CAPTCHA is found in its strength in resisting automatic adversarial attacks, and it has many applications for practical security, including free email services, online polls, search engine bots, preventing dictionary attacks, worms and spam [4]. CaRP is a combination of both a CAPTCHA and a graphical password scheme. CaRP overcome a number of security issues, such as relay attacks, online guessing attacks, and, if combined with CAPTCHA and graphical password, shoulder-surfing attacks. CaRP is click-based graphical passwords, where order of clicks on an image is used to get a new password. Unlike other click-based graphical passwords, images used in CaRP are used to generate CAPTCHA challenges, and for every login attempt 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. We point out research direction in this area. We also try to answer our CaRP as secured as graphical passwords and text based passwords. Survey will be useful for information security researchers and practitioners who are interested in finding an alternative to graphical authentication methods.

II. RELATED WORK

A. *CAPTCHA*

A CAPTCHA is a program that can generate and grade tests that: (A) most humans can pass, but (B) current computer programs cannot pass. Such a program can be used to differentiate humans from computers [5]. There are two types of visual CAPTCHA: text CAPTCHA and Image-Recognition CAPTCHA (IRC).CAPTCHA can be circumvented through relay attacks whereby CAPTCHA challenges are relayed to human solvers [1].

B. *GRAPHICAL PASSWORD*

Graphical password schemes have been proposed as a possible alternative to alphanumeric schemes, motivated partially by the fact that humans can remember images easily than text; psychological studies supports such assumption [8]. Images are generally easier to be remembered than text. 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 (presumed) advantages, there is a increasing interest in graphical password. In

Manuscript Received on November 2014.

Prof. Jayshree Ghorpade, Department of Computer Engineering, MITCOE, Pune, India.

Shamika Mukane, Department of Computer Engineering, MITCOE, Pune, India.

Devika Patil, Department of Computer Engineering, MITCOE, Pune, India.

Dhanashree Poal, Department of Computer Engineering, MITCOE, Pune, India.

Ritesh Prasad, Department of Computer Engineering, MITCOE, Pune, India.

addition to web log-in applications and workstation, graphical passwords have also been applied to mobile devices and ATM machines [6].

III. THE SURVEY

Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu [1] proposed CaRP scheme. In CaRP i.e. CAPTCHA as gRaphical Passwords, CAPTCHA and graphical password is combined and used as a single entity for authentication. The CaRP schemes are actually click-based graphical passwords with the CAPTCHA technique used in a way that a new image is generated for every login attempt even for the existing user just as CAPTCHAs change everytime. CaRP uses an alphabet set. Instead of actual characters, visual objects i.e. a visual depiction of alphanumeric characters or might be some objects is used for the CaRP image generation which actually turns out to be a CAPTCHA challenge. Noticable difference between normal CAPTCHA and CaRP images is that all objects of an alphabet set for a CaRP scheme are included in every image challenge unlike normal CAPTCHAs where only a part of alphabet set is used. Many CAPTCHA schemes can be converted to CaRP schemes, as described in the next subsection. On the basis of the memory tasks in memorizing and entering a password, classification of CaRP schemes can be done as follows: recognition based and recognition-recall. The second scheme i.e. recognition – recall CaRP is a new category which works by 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. It retains the advantages of both schemes i.e. recognition advantage of being easy for human memory and the cued-recall advantage of a large password space [1].

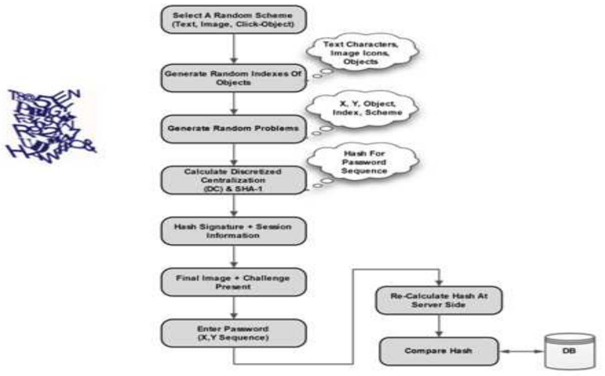

Select A Random Scheme (Text, Image, Click-Object)
Text Characters, Image Icons, Objects
Generate Random Indexes Of Objects
X, Y, Object, Index, Scheme
Generate Random Problems
Hash For Password Sequence
Calculate Discretized Centralization (DC) & SHA-1
Hash Signature + Session Information
Final Image + Challenge Present
Enter Password (X,Y Sequence)
Re-Calculate Hash At Server Side
Compare Hash
DB

Fig. 1. Flowchart of Basic CaRP Authentication of the Proposed Architecture

Step 1: Enter ID and send it to Authentication server AS.
Step 2: AS Stores a salt and hash value H(p, s) for each ID . p is the user password and it is stored.
Step 3: Upon receving login request, AS generates a CARP image. It records location of charcters or animals in image and the image is sent to the user.
Step 4: User Clicks the Password.
Step 5: Co-ordinates of points are recorded are sent to AS.
Step 6: AS maps these Co-ordinates & recovers clickable points of object p, that user clicked.
Step 7: Then AS retrieves salt s of account &calculate its hash value with salt using alsorithm like SHA-1.
Step 8: IT compares result with hash value stored for the a/c.
Step 9: Authentication is successful if and only if the two hash value matched

- ***RECOGNITION BASED CaRP***

A. CLICKTEXT

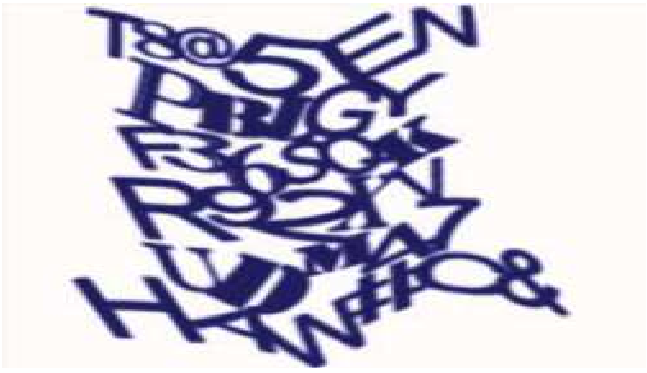


Fig. 2. ClickText CaRP Scheme [1]

ClickText is a recognition-based CaRP scheme. It uses text CAPTCHA as its underlying principle. Alphabet set of ClickText comprises alphanumeric characters. A ClickText password is a series of characters in the alphabet, e.g., ρ =“DE@F2SK78”, which is similar to a text password. A ClickText image is different from usual CAPTCHA as here all the characters of alphabet set are to be included in the image. The underlying CAPTCHA engine generates such CaRP image. When image is generated, each character’s location in the image is recorded which would be used in authentication. Characters can be arranged randomly on 2D space in these images which differs from text CAPTCHA challenges where characters are typically ordered from left to right in order for users to type them sequentially [1].

B. CLICKANIMAL

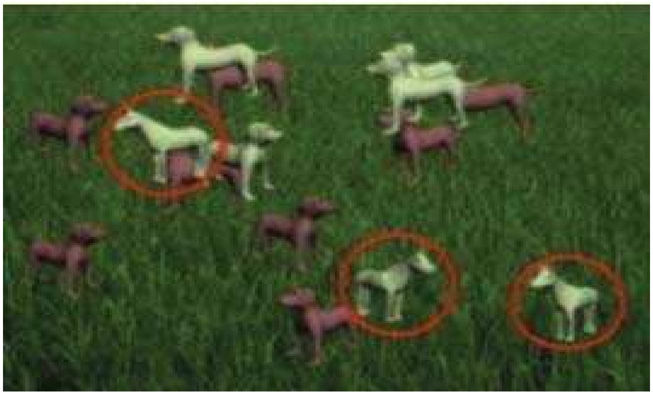
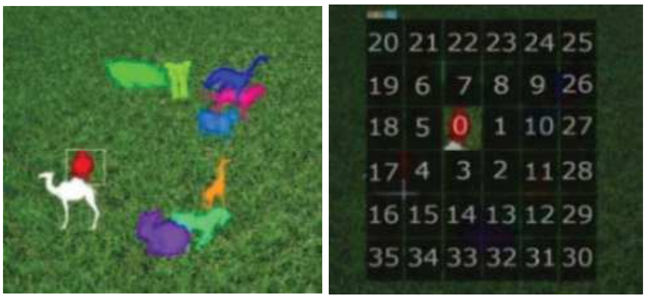


Fig. 3. ClickAnimal CaRP Scheme [1]

ClickAnimal is also a recognition-based CaRP scheme. It has an alphabet of similar animals such as dog, horse, pig, etc. The password in this scheme is a sequence of animal names such as ρ = “Cat, Dog, Horse,Turkey,….”. One or more models are built for every animal. The CAPTCHA generation process wherein 3D models are used to get 2D models by applying different views, colors, lightning effects, textures, and optionally distortions are used for generating the ClickAnimal image. The resulting 2D animals are then arranged on a cluttered background like grasslands. 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 [1].

C. ANIMALGRID



20	21	22	23	24	25
19	6	7	8	9	26
18	5	0	1	10	27
17	4	3	2	11	28
16	15	14	13	12	29
35	34	33	32	31	30

Fig. 4. A Click Animal Image (Left) and 6×6 Grid (Right) Determined by Red Turkey's Bounding Rectangle [1]

In order to resist human guessing attacks, a sufficiently-large effective password space should be present for CaRP schemes. If the ClickAnimal scheme be combined with grid-based graphical passwords, its password space can be increased. The grid can be made depending on the size of the selected animal. For authentication process, 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. 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].

IV. DISCUSSION

- *Are CaRP as secured as graphical passwords and text based passwords?*

A. The Underlying CAPTCHA Security

Usually a CAPTCHA challenge might contain about 5 to 8 characters. A CaRP image on the other hand might contain about 30 or more characters. The complexity to break a Click-Text image is about α^{30} P(N)/(α^{10}P(N)) = α^{20} times the complexity to break a CAPTCHA challenge generated by its underlying CAPTCHA scheme[1]. Thus we can get to the conclusion that the CaRP ClickText image is much harder to break than its underlying CAPTCHA scheme. As a framework of graphical passwords, CaRP does not rely on any specific CAPTCHA scheme. If one CAPTCHA scheme is broken, a new and more robust CAPTCHA scheme may appear and be used to construct a new CaRP scheme.

B. Online Guessing Attacks

The trial and error process is executed automatically in automatic online guessing attacks. However, dictionaries can be constructed manually. Such attacks can find a password only probabilistically without considering the number of trials. If a password guess in the trials is the correct one, the trial still has a lower chance of succeeding because a machine might not recognize the objects of CaRP in order to enter the correct password. This is different than the online guessing attacks on existing deterministic graphical passwords where each trial can determine if the tested password guess is the correct password or not. Also, with targeted passwords in the dictionary, attacking existing graphical passwords is successful for brute-force or dictionary attacks.

C. Shoulder-Surfing Attacks

If graphical passwords are used in public places there are chances of shoulder-surfing attacks taking place. CaRP is not robust to shoulder-surfing attacks by itself. However, combined with certain dual-view technology, CaRP can thwart shoulder-surfing attacks.

- *4.2. Is CaRP vulnerable to relay attacks?*

There are various ways to carry out relay attacks. Considering CAPTCHA challenges on websites to be hacked, one way of attack is to have human surfers solve the challenges to continue surfing the Website. Another way is having relayed to sweatshops where humans are hired to solve CAPTCHA challenges given small payments. 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. Therefore it would be unlikely to get a large number of unwitting people to mount human guessing attacks on CaRP. In addition, human input obtained by performing a CAPTCHA task on a CaRP image is useless for testing a password guess [1].

V. CONCLUSION

The paper conducts a comprehensive survey of CAPTCHA as Graphical Password schemes. CaRP is a combination of both a CAPTCHA and a graphical password scheme. CaRP schemes are classified as Recognition-Based CaRP and Recognition-Recall CaRP. We have discussed Recognition-Based CaRP which include ClickText, ClickAnimal and AnimalGrid techniques in this paper. Current graphical password techniques are an alternative to text password but are still not fully secure. As a framework, CaRP does not rely on any specific CAPTCHA scheme. When one CAPTCHA scheme is broken, a new and more secure one may appear and be converted to a CaRP scheme. Due to reasonable security and usability and practical applications, CaRP has good potential for refinements. 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.

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

[2] Matthew Dailey, Chanathip Namprempre,"A Text-Graphics Character CAPTCHA for Password Authentication"

[3] T. S. Ravi Kiran, Y. Rama Krishna, "Combining CAPTCHA and graphical passwords for user authentication" , International Journal of Research in IT & Management, Volume 2, Issue 4 (April 2012) (ISSN 2231-4334)

[4] Liming Wang, Xiuling Chang, Zhongjie Ren, Haichang Gao, Xiyang Liu, Uwe Aickelin, "Against Spyware Using CAPTCHA in Graphical Password Scheme"

[5] Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford, "CAPTCHA: Using Hard AI Problems For Security"

[6] Xiaoyuan Suo, Ying Zhu, G. Scott. Owen, "Graphical Passwords: A Survey", Department of Computer Science Georgia State University