IPHV8I1068X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

GRAPHICAL PASSWORD AUTHENTICATION USING CLICK POINTS AND CAPTCHA

[#1]Dr.GORANTLA PRABHAKARA RAO, Associate Professor,
[#2]Dr.B .SHASIDER , Professor ,
Department of Computer Science & Engineering,
[#1]SCIENT INSTITUTE OF TECHNOLOGY, HYDERABAD ,TELENGANA, INDIA.
[#2]MAHAVEER INSTITUTE OF TECHNOLOGY, HYDERABAD ,TELENGANA, INDIA.

Abstract: CAPTCHA is a computer program , it stands for (completely atomated public turning test to tell computers and human apart, which humans can pass but computer programs can't. Now a days secuirty is the major task from protecting any type of attacks. In this project, we propose a new security primitive based on hardware AI problems, namely, graphical password systems built on top of Captcha technology, we call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme. In CaRP addresses a number of security problems altogether, those are online guessing attacks, relay attacks, misbehavior attacks and, if combined with dual-view technologies, shoulder-surfing attacks. with using CaRP password can found only probabilistically by automatic online guessing attacks even if the password is in the search set. it also offers a novel approach to address the well-known image hotspot problem in popular graphical password systems. CaRP is not a quick fix, but it offers reasonable security and usability and appears to fit well with some exact applications for improving online security.

Index Terms: ***Passwords, Graphical password, attacks,captcha, graphical security, caRP.***

I. INTRODUCTION

The basic task in security is to create cryptographic primitives based on hard and mathematical problems that are computationally intractable with all the applications. For example, the problem of integer factorization is basic to the RSA publickey cryptosystem and the Rabin encryption technique. The discrete logarithm problem is fundamental to the encryption, the Diffie-Hellman key exchange,and the Digital Signature Algorithm, is used for the elliptic curve cryptography and so on. Using the basic hard AI (Artificial Intelligence) problems for security methods, initially proposed, is an exciting new prototype. Under this prototype, the most notable primitive invented is Captcha, which different human users to computers by presenting a challenging task, i.e., a puzzle,that beyond the accessing capability of computers but easy for humans. Captcha is a standard Internet security technique to secure online email and other services. In this new protocol has achieved a limited success ratio as compared with the cryptographic methods based on hard math problems and their wide applications.

Captcha is intended from users to computers by presenting a challenging task, i.e., a puzzle Captcha is now a very high standard Internet security technique to protect online email , user data and other services from being abused by bots.The CaRP is click point based graphical passwords, where a set of snaps on an image is used to derive a password as a click point .

In this paper, we propose a security primitive based on hard AI problems, namely, a novel family of graphical password systems including Captcha technology, which we call CaRP (Captcha as gRaphical Passwords).

Classification of CaRP is simple and easy but generic. the CaRP can have multiple instantiations. In theory, any Captcha scheme access on multiple-object classifications are converted to a CaRP scheme. We represent CaRPs built on text Captcha and identification of image Captcha. One of them is a text CaRP where as a password is a sequence order set of characters like a text, numeric passwords, but entered by clicking the right character or number sequence on

CaRP images. the multiple logon attempts do not work as well for two reasons:

1) It finds denial-of-service attacks which are exploited to lock highest bidders out in finalstep minutes of eBay auctions [12]) that incurs expensive help desk costs for account reactivation and re-usability.

2) the graphical password attacks where access break into any account from than specific or multiple accounts , and try to access the each password candidate on multiple accounts to ensure that the wrong no of activities, that are below the threshold value to avoid triggering account lockout.

CaRP require to solving a Captcha challenge in every login. The usability and mitigation of CaRP images at difficulty level based on the login history of the account. the CaRP scenario includes:

1). The CaRP applied on touch screen devices where typing on passwords is confuse, esp.for the secure internet applications such as e-banks, e-transactions.most of the e-banking systems have applied Captcha as user login.For example, ICBC (www.icbc.com.cn), the largest bank in the world,it requires solving a Captcha challenge for every online login attempt for the users.

2). CaRP increases spammer's and operating cost, thus helps to reduce spam mails. For an mail server provider deploys CaRP, spam bot cannot log in to mail account if if it knows the correct password.Human involvements compulsory to access and activate account. If CaRP combine with the policy to reduce the spam traffic.

II. RELATED WORK

A. Graphical Passwords:

The most of the graphical password schemes or techniques have been suggested. Graphical Password Scheme classified into three types according to the task involved in learning and entering passwords: *recognition, remembrance, and indicated recall.*

- Recognition based scheme requires to identifying the visual objects belonging to a password tasks.
- A remembrance-based scheme requires a user to regenerate the same interaction result without any extra values. The first proposed recall based scheme is Draw-A-Secret (DAS). In a Indicted-recall scheme, it is help to solve the hard AI problems.
- Visual Captcha two types they are, transcript Captcha and Image-Recognition Captcha(IRC).Transcript Captcha relay on the difficulty of character identification and which is expensive and hard to memorize enter a password.

B. Captcha

Captcha depends on the gap between the user and bots in solving the hard AI problems. Visual Captcha two types they are, transcript Captcha and Image-Recognition Captcha(IRC).Transcript Captcha relay on the difficulty of character identification and which is expensive and hard to memorize enter a password.

C. Captcha in Authentication

It was introduced for use the both Captcha and password in a user authentication protocol, we call Captcha-based Password Authentication (CbPA) protocol, is used for counter real time dictionary attacks or malicious attacks.

D. Security

An authentication method is must provide security for it's intended environment, else it fails to meet the main goal. In Proposed system should at minimum evaluate against common attacks to determine it's safety and security.we classify the knowledge based authentication into two categories, Guessing and Capture attacks. In the guessing attack , attacker able to search through the entire password space, or predict higher probability passwords. so the number of guesses are acceptable is high. guessing attacks may conduct online or offline if some variable text is used to correctness of the gusses.

Authentication systems are user choice for prevent guessing attacks. password capture attacks involve directly through the password. The malwares are common forms for capture attacks. malware types can access the website information for access the data from database.

IPHV8I1068X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

III. CAPTCHA AS GRAPHICAL PASSWORDS

A. Thwart Guessing Attacks in a guessing attack, a password guess tested in a failure trail is establish wrong and excluded from success trails. Mathematically , let S be the set of password guesses before trial, ρ is the password to find, T denotes a trial where Tn denote the n-th trial, and p(T = ρ) be the probability that ρ is tested in trial T. Let En be the set of guess passwords tested in trials up to (including) Tn. The guessing password to be tested in n-th trial Tn is from set S\En−1,i.e., the relative complement of En−1 in S memorize and enter a password.

B. CaRP:

In CaRP method, a new image is generated for every login attempt,even for the same user login also. CaRP uses an alphabet or character set of visual objects e.g(alphanumerical characters, similar animals, similar icons) to generate a CaRP, image, another taks of Captcha.

C. Converting Captcha to CaRP

In this principle, any visual Captcha scheme is used to recognizing two or more predefined types of objects can be converted to a CaRP. All text Captcha structures and most IRCs meet this requirement for visual captcha.

D. User Authentication With CaRP Schemes

Assume that CaRP schemes are used for protection between clients and the authentication server through Transport Layer Security (TLS)

IV. RECOGNITION-BASED CaRP:

In this method type CaRP, a password is a sequence of visual objects in the alphabets for detecting confusion.

A. ClickText:

ClickText is a recognition-based CaRP patterns built on top of transcript Captcha. Its alphabet includes characters without any confusing characters at visual level. For example, Letter “O” and digit “0” may look like similar for confusion in CaRP images, and thus one or more characters should be excluded from the alphabets. A ClickText password is an order bases arrangement of characters in the script based, e.g., ρ =“AB#6CD17”, it is related to a text password. It is different from text Captcha in characters are usually ordered from left to right. in order for users to type them correctly as per order. ClickText image with an set of alphabet 33 characters. In entering a password, the user images on this image the characters in the password, in the same order as per given pattern, for the above example the character set is “A”, “B”, “#”, “6”,“C”, “D”, “1”, and then “7” for password ρ = “AB#6CD17”.

Figure 1. Click Text image with 33 characters [1].

B. ClickAnimal

ClickAnimal is a recognition-based CaRP pattern is used with the anilmal names such as dog, horse, cat, Character identification is required in locating clickable points on a TextPoints image although the clickable points are known for each character. This task outside a bot’s capability.

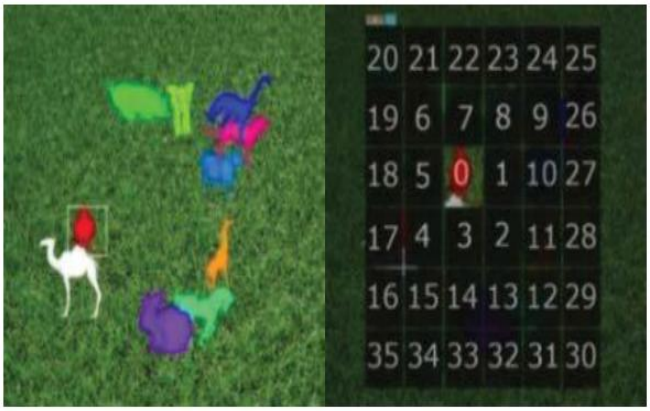

Figure 2. Click Animal images (left) and 6x6 grid (right) [1].

IPHV8I1068X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

C. Animal Grid

The number of similar animals is less than the number of offered characters. Click Animal has a small alphabet, and password space is lesser, than Click Text. Animal Grid's password space can be increased by aggregating with the grid based liable on the size of selected animal with grid based graphical password.

Figure : 3. Animal Grid

V. PROPOSED METHOD

Our proposed method is based on Recognition Technique. in this we use three different group of images is used in that. 1. Famous people 2. Famous places 3. Reputed company name.Every group contains 25 images.user have to choose one image from group at the time of registration phase. the system provides the security against dictionary attack, brute force attack,shoulder surfing attack , during graphical password.

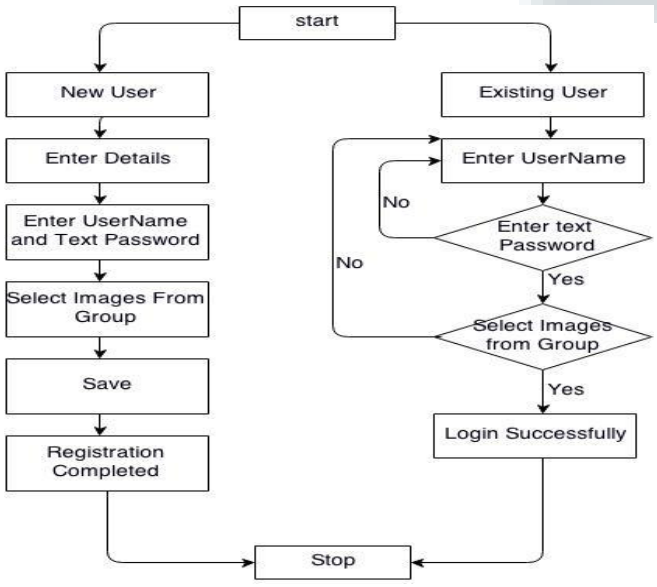

Figure: 4. Proposed System Architecture

VI. SECURITY MECHANISM

A. Security of Captcha:

The security model in captcha, identifying objects in CaRP images, A captcha typically contains 6 to 10 characters, the CaRP image usually contains minimum 30 or more characters.

B. On-line Guessing Attacks:

In online attacks, the trails and the error process is performed automatically where the dictionaries accessed manually.

C. Human Guessing Attacks

The human predicting attacks, users are tried with the individual passwords and the error process.humans are slower than the system in rising of guessing attacks.

D. Relay Attack

Relay attacks may perform in several methods. Captcha tasks can be hacked many websites and controlled by oppositions to have human surfers solve the challenging tasks in order to surfing websites.

E. Shoulder-Surfing Attacks

Shoulder-surfing attacks are a entered in a public place such as bank ATM Machines. CaRP is not hardy to shoulder surfing attacks by itself.

VII. BALANCE OF USABILITY AND SECURITY

The Designs of CaRP across the common devices , the usability in smart phones and computers studies 400×400 images.

A. Alphabet Size

The size of the alphabet expanding the large spaces alphabet size of larger password space, and thus is more protected, but also leads to more complex CaRP images.

B. Advanced Mechanisms

Captcha challenge addition to entering a password under certain conditions. the scheme applies a Captcha the number of failed login attempts has reached the threshold value.

VIII.CONCLUSION

In this paper we have suggested CaRP, a security method depend on hard AI problems. a password of CaRP can be found automatic online guessing attack, which includes brute force attacks, the

graphical password arrangements lack. it predicts the real-time scenarios attacks.

Overall , our work completely step forward in the paradigm of using hard AI problems for security. the security and usability improvements, CaRP has easy to do modifications , which is used for further future work. Carp is motivating to new discoveries of hard AI based security primitives.

REFERENCES

[1] S. Chiasson, and P. C. van Oorschot,"Graphical passwords:Learning from the first twelve years," ACM Comput. Surveys, vol. 44,no. 4, 2012.
[2].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 SecuritySymp.*, 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 PrivacySecurity*, 2007, pp. 20–28.
[9] J. Thorpe and P. C. van Oorschot, "Humanseeded attacks and exploiting hot potsingraphical passwords," in *Proc. USENIX Security*, 2007,pp. 103–118.
[10] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on passpointsstyle 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 AttackeBayAccounts*[Online].Available:http://www.zdnet.co.uk/news/networking/2002/03/26/hackersattack-ebay-accounts 2107350/
[13] HP TippingPoint DVLabs, Vienna, Austria. (2010). *Top Cyber Security Risks Report, SANS InstituteandQualysResearchLabs*[Online].Available: http://dvlabs.tippingpoint.com/toprisks2010
[14] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in *Proc. ACM CCS*, 2002, pp. 161–170.
[15] 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.

AUTHOR'S PROFILE:

[1].Dr. G.PRABHAKARA RAO, Working as Associate Professor in Computer Science and Engineering, Scient Institute Of Technology, Hyderabad ,Telengana, India.

[2]. Dr.B .SHASIDER, Professor , Department of Computer Science & Engineering, MAHAVEER INSTITUTE OF TECHNOLOGY, HYDERABAD ,TELENGANA, INDIA.