International Journal for Innovative
Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 21 July 2017. Link :
http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-5

Title:- Captcha As Graphical Passwords -A New Security Primitive Based On Hard Ai Problems

Page Numbers:- 2007 - 2012

Paper Authors

***CHIRAMANA JANARDHAN, M .HYMAVATHI**

***Department of CSE, QCET, Nellore, AP, India**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Approvals We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

CAPTCHA AS GRAPHICAL PASSWORDS -A NEW SECURITY PRIMITIVE BASED ON HARD AI PROBLEMS

CHIRAMANA JANARDHAN, Mrs. M HYMAVATHI

[1]PG Scholar, Dept of CSE, QCET,Nellore, AP, India.
[2]Associate Professor, Dept of CSE, QCET,Nellore, AP, India.

ABSTRACT

Many security primitives are based on hard mathematical problems. Using hard AI problems for security is emerging as an exciting new paradigm, but has been under-explored. In this paper, we present a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. Notably, a CaRP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. CaRP also offers a novel approach to address the well-known image hotspot problem in popular graphical password systems, such as Pass Points, that often leads to weak password choices. CaRP is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security.

1. INTRODUCTION

Computer security (Also known as cyber security or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computercannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

II.EXISTING SYSTEM:

The most notable primitive invented is Captcha, which distinguishes human users from computers by presenting a challenge, i.e., a puzzle, beyond the capability of computers but easy for humans. Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots.

2.1.DISADVANTAGES OF EXISTING SYSTEM:

This existing paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications.

III. PROPOSED SYSTEM:

In this paper, we present a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP).

CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of security problems altogether, such as online guessing attacks,

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks.

3.1.ADVANTAGES OF PROPOSED SYSTEM:

CaRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services.

CaRP also offers protection against relay attacks, an increasing threat to bypass Captchas protection.

IV.LITERATURE SURVEY

1. On predictive models and user drawn graphical passwords

AUTHORS: P. C. van Oorschot and J. Thorpe

In commonplace text-based password schemes, users typically choose passwords that are easy to recall, exhibit patterns, and are thus vulnerable to brute-force dictionary attacks. This leads us to ask whether other types of passwords (e.g., graphical) are also vulnerable to dictionary attack because of users tending to choose memorable passwords. We suggest a method to predict and model a number of such classes for systems where passwords are created solely from a user's memory. We hypothesize that these classes define weak password subspaces suitable for an attack dictionary. For user-drawn graphical passwords, we apply this method with cognitive studies on visual recall. These cognitive studies motivate us to define a set of *password complexity factors* (e.g., reflective symmetry and stroke count), which define a set of classes. To better understand the size of these classes and, thus, how weak the password subspaces they define might be, we use the "Draw-A-Secret" (DAS) graphical password scheme of Jermyn et al. [1999] as an example. We analyze the size of these classes for DAS under convenient parameter choices and show that they can be combined to define apparently popular subspaces that have bit sizes ranging from 31 to 41—a surprisingly small proportion of the full password space (58 bits). Our results quantitatively support suggestions that user-drawn graphical password systems employ measures, such as graphical password rules or guidelines and proactive password checking.

2.Modeling user choice in the PassPoints graphical password scheme

AUTHORS:A. E. Dirik, N. Memon, and J.-C. Birget We develop a model to identify the most likely regions for users to click in order to create graphical passwords in the PassPoints system. A PassPoints password is a sequence of points, chosen by a user in an image that is displayed on the screen. Our model predicts probabilities of likely click points; this enables us to predict the entropy of a click point in a graphical password for a given image. The model allows us to evaluate automatically whether a given image is well suited for the PassPoints system, and to analyze possible dictionary attacks against the system. We compare the predictions provided by our model to results of experiments involving human users. At this stage, our model and the experiments are small and limited; but they show that user choice can be modeled and that expansions of the model and the experiments are a promising direction of research.

3.Securing passwords against dictionary attacks

AUTHORS:B. Pinkas and T. Sander

The use of passwords is a major point of vulnerability in computer security, as passwords are often easy to guess by automated programs running dictionary attacks. Passwords remain the most widely used authentication method despite their well-known security weaknesses. User authentication is clearly a practical problem. From the perspective of a service provider this problem needs to be solved within real-world constraints such as the available hardware and software infrastructures. From a user's perspective user-friendliness is a key requirement. In this paper we suggest a novel authentication scheme that preserves the advantages of conventional password authentication, while simultaneously raising the costs of online dictionary attacks by orders of magnitude. The proposed scheme is easy to implement and overcomes some of the difficulties of previously suggested methods of improving the security of user authentication schemes. Our key idea is to efficiently combine traditional password authentication with a challenge that is very easy to answer by human users, but is (almost) infeasible for automated programs attempting to run dictionary attacks. This is done without affecting the usability of the system. The proposed scheme also provides better protection against denial of service attacks against user accounts.

3.Revisiting defenses against large-scale online password guessing attacks

AUTHORS:M. Alsaleh, M. Mannan, and P. C. van Oorschot

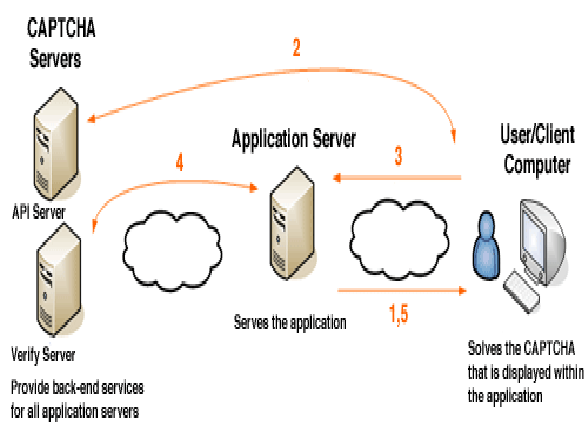
Brute force and dictionary attacks on password-only remote login services are now widespread and ever increasing. Enabling convenient login for legitimate users while preventing such attacks is a difficult problem. Automated Turing Tests (ATTs) continue to be an effective, easy-to-deploy approach to identify automated malicious login attempts with reasonable cost of inconvenience to users. In this paper, we discuss the inadequacy of existing and proposed login protocols designed to address large-scale online dictionary attacks (e.g., from a botnet of hundreds of thousands of nodes). We propose a new Password Guessing Resistant Protocol (PGRP), derived upon revisiting prior proposals designed to restrict such attacks. While PGRP limits the total number of login attempts from unknown remote hosts to as low as a single attempt per username, legitimate users in most cases (e.g., when attempts are made from known, frequently-used machines) can make several failed login attempts before being challenged with an ATT. We analyze the performance of PGRP with two real-world data sets and find it more promising than existing proposals.

3.Cognitive authentication schemes safe against spyware

AUTHORS:D. Weinshall

Can we secure user authentication against eavesdropping adversaries, relying on human cognitive functions alone, unassisted by any external computational device? To accomplish this goal, we propose challenge response protocols that rely on a shared secret set of pictures. Under the brute-force attack the protocols are safe against eavesdropping, in that an observer who fully records any feasible series of successful interactions cannot practically compute the user's secret. Moreover, the protocols can be tuned to any desired level of security against random guessing, where security can be traded-off with authentication time. The proposed protocols have two drawbacks: First, training is required to familiarize the user with the secret set of pictures. Second, depending on the level of security required, entry time can be significantly longer than with alternative methods. We describe user studies showing that people can use these protocols successfully, and quantify the time it takes for training and for successful authentication. We show evidence that the secret can be effortlessly maintained for a long time (up to a year) with relatively low loss.

V.SYSTEM ARCHITECTURE:



VI.MODULES:-

- Graphical Password
- Captcha in Authentication
- Overcoming Thwart Guessing Attacks
- Security Of Underlying Captcha

6.1.MODULES DESCRIPTION:-

1.Graphical Password:

In this module, Users are having authentication and security to access the detail which is presented in the Image system. Before accessing or searching the details user should have the account in that otherwise they should register first.

2.Captcha in Authentication:

In this module we use both Captcha and password in a user authentication protocol, which we call

Captcha-based Password Authentication (CbPA) protocol, to counter online dictionary attacks. 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.

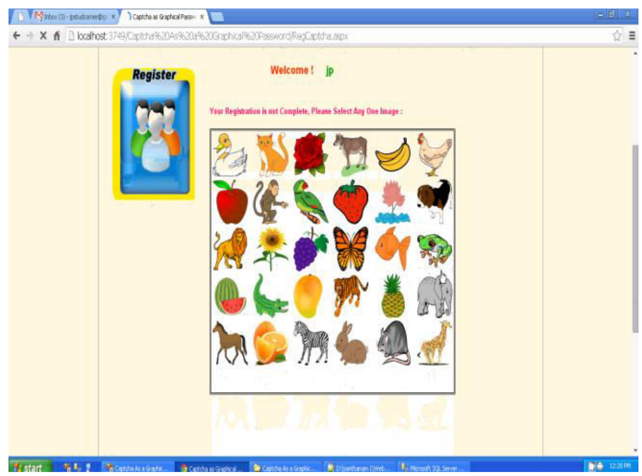
3.Overcoming Thwart Guessing Attacks:

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. 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. In this paper, we distinguish two types of guessingattacks: automatic guessing attacksapply an automatic trial and error process but *S* can be manually constructed whereas human guessing attacksapply a manual trial and error process.

4.Security of Underlying Captcha:

Computational intractability in recognizing objects in CaRP images is fundamental to CaRP. Existing analyses on Captcha security were mostly case by case or used an approximate process. No theoretic security model has been established yet. Object segmentation is considered as a computationally expensive,combinatorially-hard problem, which modern text Captcha schemes rely on.

VII.Simulation Results:



CONCLUSION:

We have proposed CaRP, a new security primitive relyingon unsolved hard AI problems. CaRP is both a Captcha anda graphical password scheme. The notion of CaRP introducesa new family of graphical passwords, which adoptsa new approach to counter online guessing attacks: a newCaRP image, which is also a Captcha challenge, is usedfor every login attempt to make trials of an online guessingattack computationally independent of each other. A passwordof CaRPcan be found only *probabilistically* by automaticonline guessing attacks including brute-force attacks, a desiredsecurity property that other graphical password schemes lack.Hotspots in CaRP images can no longer be exploited to mountautomatic online guessing attacks, an inherent vulnerability inmany graphical password systems. CaRP forces adversariesto resort to significantly less efficient and much more costlyhuman-based attacks. In addition to offering protection fromonline guessing attacks, CaRP is also resistant to Captcharelay attacks, and, if combined with dual-view technologies,shoulder-surfing attacks. CaRP can also help reduce spamemails sent from a Web email service.

Our usability study of two CaRP schemes we haveimplemented is encouraging. For example, more participantsconsidered AnimalGrid and ClickText easier to use thanPassPoints and a combination of text password and Captcha.Both AnimalGrid and ClickText had better password memorabilitythan the conventional text passwords. On the other hand,the usability of CaRP can be further improved by using imagesof different levels of difficulty based on the login history ofthe user and the machine used to log in. The optimal tradeoffbetween security and usability remains an open question forCaRP, and further studies are needed to refine CaRP for actualdeployments.

Like Captcha, CaRP utilizes unsolved AI problems.However, a password is much more valuable to attackers thana free email account that Captcha is typically used to protect.Therefore there are more incentives for attackers to hack CaRPthan Captcha. That is, more efforts will be attracted to thefollowing win-win game by CaRP than ordinary Captcha:If attackers succeed, they contribute to improving AI byproviding solutions to open problems such as segmenting2D texts. Otherwise, our system stays secure, contributingto practical security. As a framework, CaRP does not relyon any specific Captcha scheme. When one Captcha schemeis broken, a new and more secure one may appear and beconverted to a CaRP scheme.Overall, our work is one step forward in the paradigm ofusing hard AI problems for security. Of reasonable securityand usability and practical applications, CaRP has goodpotential for refinements, which call for useful future work.More importantly, we expect CaRP to inspire new inventionsof such AI based security primitives.

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 designand 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 ofgraphical 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 passwordsystem," *Int. J. HCI*, vol. 63, pp. 102–127, Jul. 2005.

[6] P. C. van Oorschot and J. Thorpe, "On predictive models and userdrawngraphical 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 thepasspoints graphical

password scheme," in *Proc. Symp. Usable PrivacySecurity*, 2007, pp. 20–28.

[9] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploitinghot spots in graphical passwords," in *Proc. USENIX Security*, 2007,pp. 103–118.

[10] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automatedattacks on passpoints-style 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 clickbasedgraphical passwords," *J. Comput. Security*, vol. 19, no. 4,pp. 669–702, 2011.

[12] T. Wolverton. (2002, Mar. 26). *Hackers Attack eBay Accounts*[Online]. Available: http://www.zdnet.co.uk/news/networking/2002/03/26/hackers-attack-ebay-accounts-2107350/

[13] HP TippingPointDVLabs, Vienna, Austria. (2010). *Top Cyber SecurityRisks Report, SANS Institute and Qualys Research Labs* [Online].Available: http://dvlabs.tippingpoint.com/toprisks2010

[14] B. Pinkas and T. Sander, "Securing passwords against dictionaryattacks," in *Proc. ACM CCS*, 2002, pp. 161–170.

[15] P. C. van Oorschot and S. Stubblebine, "On countering online dictionaryattacks with login histories and humans-in-the-loop," *ACM Trans. Inf.Syst. Security*, vol. 9, no. 3, pp. 235–258, 2006.

[16] M. Alsaleh, M. Mannan, and P. C. van Oorschot, "Revisitingdefenses against large-scale online password guessing attacks," *IEEETrans. Dependable Secure Comput.*, vol. 9, no. 1, pp. 128–141,Jan./Feb. 2012.