Current Trends in Technology and Science
ISSN: 2279-0535. Volume: V, Issue: IV

A NEW SECURITY CONCERN: CAPTCHA AS GRAPHICAL PASSWORD

Laxmi Kosariya[1], Prof. Kailash Patidar[2], Narendra Sharma[3]

PG Student, Dept. of CSE, SSSUTMS, Sehore, M.P., India[1]
Professor& Head, Dept. of CSE, SSSUTMS, Sehore, M.P., India[2]
Assistant Professor, Dept. of CSE, SSSUTMS, Sehore, M.P., India[3]

ABSTRACT: Numerous security primitives depend on hard scientific issues. Utilizing hard AI issues for security is rising as an energizing new worldview, however has been under-investigated. In this paper, we show another security primitive taking into account hard AI issues, in particular, a novel group of graphical secret key frameworks based on top of Captcha innovation, which we call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical secret word plan. CaRP addresses various security issues inside and out, for example, web speculating assaults, transfer assaults, and, if joined with double view innovations, shoulder-surfing assaults. Outstandingly, a CaRP secret word can be discovered just probabilistically via programmed internet speculating assaults regardless of the fact that the watchword is in the inquiry set. CaRP likewise offers a novel way to deal with location the understood picture hotspot issue in mainstream graphical secret key frameworks, for example, Pass Points, that regularly prompts powerless watchword decisions. CaRP is not a panacea, but rather it offers sensible security and ease of use and seems to fit well with some viable applications for enhancing online security.

Kew words— Password, Graphical Password, Password Guessing Attack, Hotspots, CaRP, Captcha, Dictionary Attack

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 technique by which computer-based systems, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned incidents and inevitable disasters. Otherwise, in the area of computer, the term security or the phrase computer security refers to techniques for ensuring that data stored in a computer cannot be accessed by any individuals without any authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is incomprehensible without a deciphering technique. A password is a secret word or phrase that gives a user access to a particular program or system.

2. LITERATURE SURVEY

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 sparks us to 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 anticipate and model a number of such classes for computer systems where passwords are created merely from a user's memory. We hypothesize that these classes define weak password subspaces suitable for a dictionary attack. For user graphical passwords, we apply this method with intellectual studies on visual recall. These cognitive studies motivate us to define a set of *password complexity factors* (e.g. stroke count), which define a set of classes. To better understand the size of these classes and, thus, how weak password subspaces they define might be use the "Draw-A-Secret" (DAS) graphical password pattern of Jermyn.

We analyze the size of these classes for DAS under convenient parameter choices and so that they can be combined to define intuitively popular subspaces that have bit sizes ranging from 31 to 41, exceptionally small proportion of the full password space (58 bits). Our results quantifiable support suggestions that user-drawn graphical password systems employ measures, such as graphical password rules or guidelines and proactive password checking. [1]

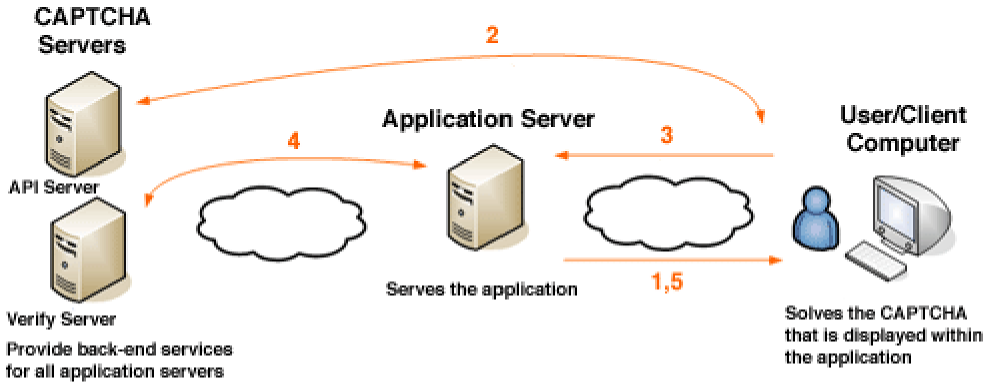
We evolve a model to find the most likely regions for users to click in order to generate graphical passwords in the PassPoints system. A PassPoints password is a sequence of points, chosen by a user in an image that is displayed on the screen. Our model presumes probabilities of likely click points; this enables us to predict the entropy of a click point in a graphical password for a given image. The model allows us to assess automatically whether a given image is well suited for the PassPoints system, and to analyze possible dictionary attacks against the system. We analyze the predictions provided by our model to results of experiments involving human users [2]. At this stage, our model and the experiments are small and limited; but they show that user preference can be modeled and that expansions of the model and the experiments are a promising direction of research.

The usage of passwords is a major point of vulnerability in computer security, as passwords are often easy to predict by automated programs by running dictionary attacks. Passwords remain the most widely used authentication method despite their well-known security vulnerabilities. User authentication is clearly a practical dilemma. From the perspective of a service provider this dilemma needs to be solved within real-world constraints such as the available hardware and software infrastructures. From a user's perspective feasibility is a key requirement. In this paper we suggest a novel authentication strategy that perpetuates the advantages of conventional password authentication, while simultaneously boosting the costs of online dictionary attacks by orders of magnitude. The proposed scheme is easy to implement and overthrown some of the difficulties of formerly suggested methods of bettering the security of user authentication schemes. Our main idea is to efficiently combine traditional password authentication with a confrontation that is very easy to answer by human users, but is (almost) infeasible for automated programs attempting to run dictionary attacks [3]. This is done without stirring the usability of the system. The proposed scheme also provides better safeguard against denial of service attacks adjacent user accounts.

3. PROBLEM IDENTIFICATION

Existing System:

The most illustrious primitive invented is Captcha, which discriminates 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 mechanism to protect emails and other services from being victimize by bots.


CAPTCHA Servers
2
Application Server
User/Client Computer
4
3
API Server
Serves the application
1,5
Verify Server
Provide back-end services for all application servers
Solves the CAPTCHA that is displayed within the application

Disadvantages of Existing System:

This existing model has achieved just a limited success in comparison with the cryptographic primitives based on hard math problems and their wide utilization.

4. PROPOSED WORK

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 address Captcha as graphical passwords (CaRP).
CaRP is both a Captcha and a graphical password mechanism. CaRP addresses a number of security threats altogether such as, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks, online guessing attacks.

Advantages of Proposed System:

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

CaRP also gives us protection against relay attacks, an increasing threat to bypass Captcha protection.

5. CONCLUSION

We have proposed CaRP, a new security primitive relying on unsolved hard AI problems. CaRP is both a Captcha and a graphical password scheme. The notion of CaRP introduces a new family of graphical passwords, which adopts a new approach to counter online guessing attacks: a new CaRP image, which is also a Captcha challenge, is used for every login attempt to make trials of an online guessing attack computationally independent of each other. A password of CaRP can be found only *probabilistically* by automatic online guessing attacks including brute-force attacks, a well suited and relevant security property that other graphical password pattern lack. Hotspots in CaRP images can no longer be exploited to mount automatic guessing attacks online, an implicit vulnerability in many graphical password systems. CaRP forces adversaries to resort to significantly less efficient and much more costly human-based attacks. In addition to offering protection from online guessing attacks, CaRP is also rebellious to Captcha relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. CaRP can also help reduce spam emails sent from a Web email service.

Of reasonable security and usability and practical applications, CaRP has good potential for rectification, which call for useful future work. More importantly, we expect CaRP is to trigger new inventions of such AI based security primitives.

REFERENCE:

1. P.C. van Oorschot, Julie Thorpe, School of Computer Science, Carleton University, Canada, On Predictive Models and User-Drawn Graphical Passwords, DAS Journal, 2 June 2007, https://ccls.carleton.ca/paper-archive /DAS_journal_preprint.pdf
2. A. E. Dirik, N. Memon, and J.-C. Birget, Modeling User Choice In The Passpoints Graphical Password Scheme, Symposium On Usable Privacy and Security (SOUPS) 2007, July 18-20, 2007, Pittsburgh, PA, USA. https://cups.cs.cmu.edu/soups/ 2007/proceedings/p20_dirik.pdf
3. B. Pinkas and T. Sander, Securing Passwords Against Dictionary Attacks, *Proc. ACM CCS*, 2002, pp. 161–170. http://www.pinkas.net/PAPERS/pwdweb.pdf
4. 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.
5. 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.
6. 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.
7. 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.
8. HP TippingPointDVLabs, Vienna, Austria. (2010). *Top Cyber Security Risks Report, SANS Institute and Qualys Research Labs* [Online]. Available: http://dvlabs.tippingpoint.com/topris ks2010
9. L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, “CAPTCHA:Using hard AI problems for security,” in *Proc. Eurocrypt*, 2003,pp. 294–311.
10. J. Yan and A. S. El Ahmad, “A low-cost attack on a Microsoft CAPTCHA,” in *Proc. ACM CCS*, 2008, pp. 543–554.
11. (2012, Feb.). *The Science BehindPassfaces*[Online]. Available: http://www.realuser.com/published/ ScienceBehindPassfaces.pdf