IJCSN International Journal of Computer Science and Network, Volume 6, Issue 2, April 2017
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

SecuCloud: A 3D Security Based Graphical Password Scheme to Solve Hard AI Problems and Provide Security in Cloud

[1] Sunny Solanki; [2] Rishikesh Ghulaxe; [3] Shreya Salve; [4] Vaibhav Dhok; [5] Roma Kudale

[1 2 3 4 5] Department of Computer Engineering, SKNCOE, SPPU University,
Pune, Maharashtra-411041, India.

Abstract - CAPTCHA is a technique that identifies the difference between human and bots so as to protect the user account from invariant bot attacks. Putting the benefits of hard AI problems, as well as, that of CAPTCHA technology together, a new security primitive known as Captcha as gRaphical Password (CaRP) was introduced to make the system more secure for the user providing security from various bot attacks. In this paper, we present a new and better security primitive which consists of a 3-layered graphical password scheme involving three levels of authentication for the user, i.e., in the first phase, a CAPTCHA based authentication method is used (clicks on a CAPTCHA image are stored as hash values). The second phase of authentication consists of sequence of images to be entered from a selected grid of images made available to the user. The third phase uses a click based authentication technique on an image selected by the user. Hence, in this way, the proposed system provides a 3-layer security to the client for better and more secure authentication and keeps the data secured on cloud.

Keywords – *Captcha, CaRP, Hard AI Problems, Graphical Passwords.*

1. Introduction

One of the important motives behind implementing security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable.

AI hard problems are the most difficult problems to be solved in the field of artificial intelligence making them equivalent to that of solving the central artificial intelligence problem, which is, making computers as intelligent as people. Currently, AI-hard problems also require human computation along with modern technology to be solved.

Thus, the usage of hard AI (Artificial Intelligence) problems for security, as proposed earlier, was an exciting new paradigm form the perspective of security under which the most notable primitive is Captcha, which distinguished the human users from bots by presenting them a challenge in the form of a puzzle that was difficult for the bots to solve and much easier for the humans. This innovative feature of Captcha thus enabled to provide access to online services and products to its genuine and verified users and protect them from being abused by bots. Captcha however achieved just a limited success as compared to the encryption techniques that were based on hard math problems. This motivated us to further explore the capabilities of Captcha and integrate it with the graphical password schemes based on hard AI problems so as to introduce a novel technique for password authentication that could tackle various attacks such as online guessing attacks, online dictionary attack, denial-of-service attacks, etc. This directed us towards the use of CaRP, abbreviated for Captcha as gRaphical Password, as one of the prime authentication gateway towards the designated system.

Our paper proposes a 3-layer authentication system, which uses CaRP as one of the main layers in the authentication system. In this authentication system, the first layer at the time of login would consist of Captcha image that would consist of letters and special characters. In order to gain access to the system, the user would be required to make clicks on the image corresponding to the characters with respect to the password chosen at the time of registration. For the first layer password chosen at the time of registration, corresponding hash values will be stored in the database, and accordingly at the time of login, these hash values will be matched to decide if the password is correct or not. The characters in the Captcha

image would be distorted to a certain amount by using image processing.

To avoid ambiguity between characters that the users decide by clicking on the Captcha image, we would be implementing the Centered Discretization algorithm, which proves to be a better alternative to the Robust Discretization technique.

The second layer of this authentication system consist of selecting a particular set of images from a selected grid of images made available to the user at the time of login, in the same sequence as they would have selected at the time of registration.

The third layer of authentication provides a click based graphical password authentication in which a particular click on image, selected at the time of registration, would result in successful access. This layer is accompanied by a 4-digit numerical password.

2. Related Work

Captcha as a graphical password (CaRP) is basically a new security primitive which is completely based on hard AI problems, that is, a novel family of graphical password systems which are built on top of Captcha technology. Captcha was first pioneered by two groups which were working in parallel: 1)Mark D. Lillibridge, Martin Abadi, Krishna Bharat and Andrei Z. Broder; and 2)Reshef, Rahaan and Solan in the year 1997 at AltaVista. The Captcha term was coined by Luis von ahn, Manuel Blum, Nicholas J. Hopper and John Langford in 2003. This form of Captcha requires that the user types the letters shown on the screen in the form of distorted images, sometimes it can be with the addition of an obscured sequence of letters or may be digits that appear to be on the screen.

During the prior days of internet, users wanted to make text illegible to the computers. Such people firstly could be hackers which posted about sensitive topics to online forums they thought were automatically being monitored for the keywords. To circumvent these filters, they could replace a word with look-alike characters. HELLO could become |-|3|_|_() or)-(3££0 , as well as several other variants, such that a filter could not possibly detect all of them. A password of CaRP can be detected probabilistically only just by automatic online guessing attacks which includes brute-force attacks, a desired security property that other graphical password schemes lack. CaRP forces adversaries to resort to very significantly lesser efficient and much costlier human-based attacks.

In addition to offering the protection from online guessing attacks, CaRP is also resistant to Captcha-relay attacks, and, if it gets combined with dual-view technologies, it also becomes resistant to shoulder-surfing attacks. CaRP can also help reduce the spam emails sent from a Web email service department. This technique provides smart solutions as far as password security and attacks are concerned with the help of Artificial Intelligence.

3. Motivation

Security has been one of the prime concerns when it comes to accessing online resources or an account as a whole. The most common and impactful methods of breaching security is to get unauthorized access via cracking passwords. Cracking passwords would involve any of the techniques such as dictionary attacks, online guessing attacks, shoulder surfing, etc. Solution to this problem of password cracking led to the use of hard AI problems for security which further to innovation of CAPTCHA technology. The concern with this technology was that it was merely used for the recognition of an user as a human or a bot. However, it didn't actually solve the core problem of password cracking. This led us to integrate CAPTCHA into the password authentication scheme, thus helping to tackle the main concern of bot attacks to get unauthorized access. This technology was further combined with two more levels of graphical password scheme, leading us to three levels of security for authentication schemes.

4. Different Phases and System Architecture

In our project we are using two main phases:

i. Registration Phase
ii. Authentication Phase

4.1 Registration Phase

This phase is basically the Sign-up phase that is to be used by the user if he is not registered in the system. In this phase, the user has to opt for the appropriate passwords for the 3 levels of authentication.

The first level of password will be a textual password that will be entered through the keyboard. Based on the characters entered, appropriate hash values are calculated by the system and saved in the database based on the challenge image that it generates to the user for authentication. The hash values are calculated using

SHA-1 algorithm to provide additional security to the system.

The second level of password comprises of selection of 5 graphic images from a given set that the user has to select in a particular order.

The third level comprises of selection of an image with a single unique click combined with numerical password.

4.2 Authentication Phase

This phase could be referred to as the Sign-in or Log-in phase in which the user is already registered into the system along with his credentials and other information. In this phase, the user has to pass through the 3 levels of authentication for gaining access to his/her account/resources.

It is to be noted that this phase is purely click based and does not involve any other medium of input. Also, it should be noted that the user cannot pass through next level of authentication unless and until he passes the current level by providing the appropriate password.

The first level of authentication involves a CAPTCHA image generated with rendered characters. The user has to click on the characters based on textual password entered in the registration phase.

The correct sequence of clicks on image is verified by the system by matching of the corresponding hash value generated with the hash value saved in the database that was calculated by the system for corresponding Challenge image.

An important thing to be noted here is that this CAPTCHA image is generated using the Centered Discretization [9] algorithm which makes the Discretization process easier by elimination of false accepts and false rejects and also allows for smaller tolerance regions without impacting the usability of the system.

Another aspect to be kept in mind is that for every new login session, the CAPTCHA/Challenge image generated will be different from the previous session and hence the hash values generated will also be different.

The second layer of this authentication system consist of selecting a particular set of images from a selected grid of images made available to the user at the time of login, in the same sequence as they would have selected at the time of registration.

The third layer of authentication provides a click based graphical password authentication in which a particular click on image, selected at the time of registration, would result in successful access. This layer is accompanied by a 4-digit numerical password.

All the communication between the client and the server is supported by SOAP (Simple Object Access Protocol).

In our project, passwords are not stored in databases but they are stored and retrieved by Serialization method in which the passwords are stored in the form of file format.

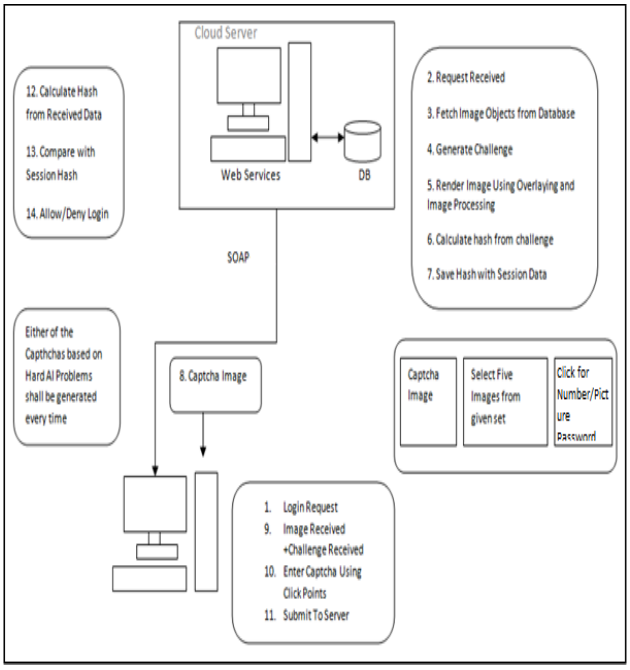

Fig. 1: Proposed Architecture

4. Conclusion and Future Scope

In the proposed system, we would be using a 3-layered graphical password scheme, with Captcha as gRaphical Password (CaRP) as one of main gateways of authentication. The correct use of image processing and AI technique leads us to provide solutions to tackle online guessing attack, dictionary attack, relay attack etc. In this system, the CAPTCHA challenge images presented to the user at the time of login have been innovatively designed and these challenge images generated will be different from the previous session. This scheme provides security as well as usability to the user. The proposed scheme can

be used in applications like payment gateways, military applications, spam mitigation etc. where confidential and sensitive data is involved.

The future research should be focused on improving the login time and memorability. The other possible extensions to the proposed scheme could be working on the implementation of CaRP schemes in virtual environment.

Also, another possible extension could be that the user would be able to set his 2nd and 3rd layer password with the help of its own set of images.

Acknowledgments

We take this great opportunity to thank everyone who has contributed to our project in some or other way. We would like to thank our project guide Prof. Roma Kudale and Prof. Shyam Kosbatwar for their guidance for developing this project.

References

[1] Vikas K. Kolekar, Milindkumar B. Vaidya "Click and Session Based-Captcha as Graphical Password Authentication Schemes for Smart Phone and Web", International Conference on Information Processing (ICIP), December 2015.

[2] Priti P. Doke, S.A Nagtilak "A Survey on CAPTCHA as Graphical Password", International Journal of Science and Research (IJSR), Volume 4 Issue 12, December 2015.

[3] R.G.Vetrivel, J.Vasanth Kishore, B. Arun Kumar, S. Thivaharan "Data Security using Carp Two Step Authentication based on Human and Hard AI Problems", IJARCCE, Volume 4 Issue 3, March 2015.

[4] Hossein Nejati, Ngai-Man Cheung, Ricardo Sosa, Dawn Chin-Ing Koh "DeepCAPTCHA: An Image CAPTCHA Based on Depth Perception", Proceedings of the 5th ACM Multimedia Systems Conference, July 2014.

[5] 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.

[6] P.R.Devale Shrikala, M. Deshmukh, Anil B.Pawar "Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme.", International Journal of Soft Computing and Engineering, Volume-3, Issue-2 May 2013.

[7] Darryl D'Souza, Phani C Polina,Roman V Yampolskyi "Avatar Captcha: Telling Computers and humans apart via face classification.", Electo/Information Technology (EIT), 2012 IEEE International Conference, May 2012.

[8] Kemal Bicakci, Nart Bedin Atalay, Mustafa Yuceel, Hakan Gurbaslar, Burak Erdeniz "Towards Usable Solutions to Graphical Password Hotspot Problem.", Computer Software and Applications Conference, 2009 (ISBN: 978-0-7695-3726-9).

[9] Sonia Chiasson, Jayakumar Srinivasan, Robert Biddle, P.C. van Oorschot "Centered Discretization with Application to Graphical Passwords.", 2009.

[10] S. Chiasson, A. Forget, R. Biddle and P. C. van Oorschot, "Influencing users towards better passwords: Persuasive cued click-points," in Proc. Brit. HCI Group Annu. Conf. People Comput., Culture, Creativity, Interaction, vol. 1, pp.121-130, 2008.