ISSN 2395-1621

A Survey On Online Security Authentication Using Visual Cryptographic

[#1]Akshay Digrase, [#2]Abhinav Vare, [#3]Sushant, [#4]Prof. Navdeep Bagga

[1]digraseakshaykumar86@gmail.com
[2]abhinav.vare@gmail.com

[#123]Department of Computer Engineering,
[#4]Prof. Department of Computer Engineering,
GHRCEM,
G.H.Raisoni College of Engineering and Management, Pune

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 underexplored. 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.

Keywords: **Graphical password, password, hotspots, CaRP, Captcha, dictionary attack, password guessing attack, security primitive.**

ARTICLE INFO

Article History

Received: 24th January 2016

Received in revised form :

24th January 2016

Accepted: 27th January, 2016

Published online :

27th January, 2016

I. INTRODUCTION

A Fundamental task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. For example, the problem of integer factorization is fundamental to the RSA public-key cryptosystem and the Rabin encryption. The discrete logarithm problem is fundamental to the ElGamal encryption, the Diffie Hellman key exchange, the Digital Signature Algorithm, the elliptic curve cryptography and so on. Using hard AI (Artificial Intelligence) problems for security, initially proposed in , is an exciting new paradigm. Under this paradigm, 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. However, this new paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications. Is it possible to create any new security primitive based on hard AI problems? This is a challenging and interesting open problem. In this paper, we introduce a new security primitive based on hard AI problems, namely, a novel family of graphical password systems integrating Captcha technology, which we call CaRP (Captcha as graphical Passwords). CaRP is click-based graphical passwords, wherea sequence of clicks on an image is used to derive a password. Unlike other click-based graphical passwords, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every login attempt. The notion of CaRP is simple but generic. CaRP can have multiple instantiations. In theory, any Captcha scheme relying on multiple-object classification can be converted to a CaRP scheme. We present exemplary CaRPs built on both text Captcha and image-recognition Captcha. One of them is a text CaRP wherein a password is a sequence of characters like a text password, but entered by clicking the right character sequence on CaRP images. CaRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online

services. This threat is widespread and considered as a top cyber security risk. Defense against online dictionary attacks is a more subtle problem than it might appear. Intuitive countermeasures such as throttling logon attempts do not work well for two reasons:

1) It causes denial-of-service attacks (which were exploited to lock highest bidders out in final minutes of eBay auctions) and incurs expensive helpdesk costs for account reactivation.

2) It is vulnerable to global password attacks whereby adversaries intend to break into any account rather than a specific one, and thus try each password candidate on multiple accounts and ensure that the number of trials on each account is below the threshold to avoid triggering account lockout. CaRP also offers protection against relay attacks, an increasing threat to bypass Captchas protection, wherein Captcha challenges are relayed to humans to solve. Koobface was a relay attack to bypass Facebook's Captcha in creating new accounts. CaRP is robust to shoulder-surfing attacks if combined with dual-view technologies.

II. RELATED WORK

A Compressive Sensing Based Secure Watermark Detection And Privacy Preserving Storage Framework

Qia Wang, Wenjun Zeng, Fellow, IEEE, and Jun Tian, Member, IEEE

Privacy is a critical issue when the data owners outsource data storage or processing to a third party computing service, such as the cloud. In this paper, we identify a cloud computing application scenario that requires simultaneously performing secure watermark detection and privacy preserving multimedia data storage. We then propose a compressive sensing (CS)-based framework using secure multiparty computation (MPC) protocols to address such a requirement. In our framework, the multimedia data and secret watermark pattern are presented to the cloud for secure watermark detection in a CS domain to protect the privacy. During CS transformation, the privacy of the CS matrix and the watermark pattern is protected by the MPC protocols under the semi-honest security model. We derive the expected watermark detection performance in the CS domain, given the target image, watermark pattern, and the size of the CS matrix (but without the CS matrix itself). The correctness of the derived performance has been validated by our experiments. Our theoretical analysis and experimental results show that secure watermark detection in the CS domain is feasible. Our framework can also be extended to other collaborative secure signal processing and data-mining applications in the cloud.

Novel Anti Phishing framework based on Visual Cryptograph

Divya James,Mintu Philip

With the advent of internet, various online attacks has been increased and among them the most popular attack is phishing. Phishing is an attempt by an individual or a group to get personal confidential information such as passwords, credit card information from unsuspecting victims for identity theft, financial gain and other fraudulent activities. Fake websites which appear very similar to the original ones are being hosted to achieve this. In this paper we have proposed a new approach named as "A Novel Anti-phishing framework based on visual cryptography "to solve the problem of phishing. Here an image based authentication using Visual Cryptography is implemented. The use of visual cryptography is explored to preserve the privacy of an image captcha by decomposing the original image captcha into two shares (known as sheets) that are stored in separate database servers(one with user and one with server) such that the original image captcha can be revealed only when both are simultaneously available; the individual sheet images do not reveal the identity of the original image captcha. Once the original image captcha is revealed to the user it can be used as the password. Using this website cross verifies its identity and proves that it is a genuine website before the end users.

Enhanced Security in Cloud Computing

Akash Mehra, Emon vuess

The cloud computing is a modern technology of storing the information or large amount of data on the internet and accessing it from there. It may happen at times that many malicious users may hack the data or vital information from the cloud, so providing security to these clouds is the major concern today.A cloud can be private or public. In this paper we will describe the multi-clouds which is the clone of the cloud so that users can access information from any one of them and it is readily available.It surveys the recent research related to single and multi-cloud and suggests possible solutions. Also in later section,we are providing security to these clouds because the research shows that cloud security has received less information in past.This paper aims at promoting the use of multi-clouds so that maximum users can make use of this technology.This paper describes how can we overcome the problems related to clouds such as making service availability,increase the response time and to prevent the system from crashing down.Most of these issues can be overcome by using the "multi-clouds" also called as "inter-clouds". This work reduces the security risks related to cloud computing that affect its users.

III.CONTRIBUTION

In CaRP, a new image is generated for every login attempt, even for the same user. CaRP uses an alphabet of visual objects (e.g., alphanumerical characters, similar animals) to generate a CaRP image, which is also a Captcha challenge. A major difference between CaRP images and Captcha images is that all the visual objects in the alphabet should appear in a CaRP image to allow a user to input any password but not necessarily in a Captcha image. Many Captcha schemes can be converted to CaRP schemes, as described in the next subsection. CaRP schemes are clicked-based graphical passwords. According to the memory tasks in memorizing and entering a password, CaRP schemes can be classified into two categories: recognition and a new category, recognition-recall, which requires 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, and retains both the recognition-based advantage of being easy for human memory and the cued-recall advantage of a large password space. Exemplary CaRP schemes of each type will be presented later.

IV.PROPOSED METHODOLOGY AND DISCUSSION

There are three parties in the proposed framework, the data holders (DH) of the potentially watermarked images, the watermark owners (WO) and the cloud (CLD) as illustrated in. The framework also requires a certificate authority (CA) to issue the public keys and CS matrix keys to certain parties of the framework. For DH (e.g., media agencies), when it collects a large volume of multimedia data from the Internet and stores their encrypted versions in the CLD, it wants to make sure those multimedia can be edited and republished legally. Watermark owners (WOs) are also the content providers who distribute their watermarked content (the watermark embedding is performed by WO before the contents are published). WOs always want to know if their contents are legally used and republished. In some scenarios, not only DH and WO care about the copyright of the multimedia data, certain CLD who offers storage services may also desire to initiate the watermark detection to check if the uploadedmultimediadata is copyright protected. For example, a CLD may choose not to provide storage services to copyright protected data illegally owned. If DH would like to use a CLD for storage or migrate the encrypted multimedia data from another cloud to this CLD, it will require the CLD to perform watermark detection on the encrypted multimedia data before providing the storage services.

V. ARCHITECTURE

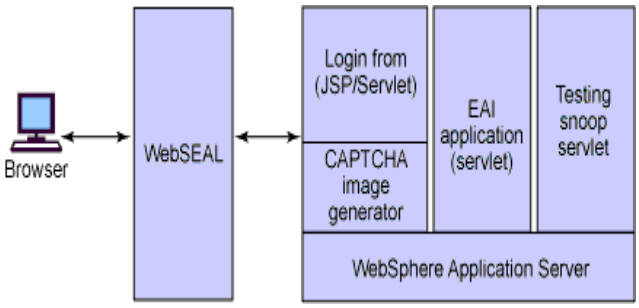

Fig 1. CAPCHA authentication Architecture

In principle, any visual Captcha scheme relyingon recognizing two or more predefined types of objects can be converted to a CaRP. All text Captcha schemes and most IRCs meet this requirement. Those IRCs that rely on recognizing a single predefined type of objects can also be converted to CaRPs in general by adding more types of objects. In practice, conversion of a specific Captcha scheme to a CaRP scheme typically requires a case by case study, in order to ensure both security and usability. We will present in Sections IV andV several CaRPs built on topof text and image-recognition Captcha schemes. Some IRCs rely on identifying objects whose types are not predefined. A typical example is Cortcha [25] which relies on context-based object recognition wherein the object to be recognized can be of any type. These IRCs cannot be converted into CaRP since a set of pre-defined object types is essential for constructing a password.

Like other graphical passwords, we assume that CaRP schemes are used with additional protection such as secure channels between clients and the authentication server through Transport Layer Security (TLS). A typical way to apply CaRP schemes in user authentication is as follows. The authentication server AS stores a salt s and a hash value $H(\rho, s)$ for each user ID, where ρ is the password of the account and not stored. A CaRP password is a sequence of visual object IDs or clickable-points of visual objects that the user selects. Upon receiving a login request, AS generates a CaRP image, records the locations of the objects in the image, and sends the image to the user to click her password. The coordinates of the clicked points are recorded and sent to AS along with the user ID. AS maps the received coordinates onto the CaRP image, and recovers a sequence of visual object IDs or clickable points of visual objects, ρ , that the user clicked on the image. Then AS retrieves salt s of the account, calculates the hash value of ρ with the salt, and compares the result with the hash value stored for the account. Authentication succeeds only if the two hash values match. This process is called the basic CaRP authentication and shown in Fig. 1. Advanced authentication with CaRP, for example, challenge-response, will be presented in Section V-B. We assume in the following that CaRP is used with the basic CaRP

authentication unless explicitly stated otherwise. To recover a password successfully, each user-clicked point must belong to a single object or a clickable-point of an object. Objects in a CaRP image may overlap slightly with neighboring objects to resist segmentation. Users should not click inside an overlapping region to avoid ambiguity in identifying the clicked object. This is not a usability concernin practice since overlapping areas generally take a tiny portion of an object.

VI. 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 desired security property that other graphical password schemes lack. Hotspots in CaRP images can no longer be exploited to mount automatic online guessing attacks, an inherent 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 resistant 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.

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,

2. 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 design and analysis of graphical passwords,” in Proc. 8th USENIX Security Symp., 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.

