Enhancing CAPTCHA Security Using Interactivity, Dynamism, and Mouse Movement Patterns

Narges Roshanbin, University of Alberta, Edmonton, Canada
James Miller, University of Alberta, Edmonton, Canada

ABSTRACT

Many existing CAPTCHAs require users to identify characters in a static image and match them with their counterparts in another image. Requiring intelligent human interaction in the matching task of these CAPTCHAs will pose a second challenge, which is straightforward for human users but difficult to emulate for Bots. In this paper, the authors develop several interactive matching tasks involving dynamic elements and demonstrate their impact on CAPTCHA security and usability in a series of tests and user studies. Their tests indicate that requiring intelligent human interaction can substantially decrease the likelihood of a CAPTCHA being broken in addition to making an attack computationally expensive. The authors’ results provide both a security and a usability benchmark for the development of interactive dual-challenge CAPTCHAs. Their proposed findings from users’ mouse movement data analysis can be readily incorporated in several types of existing CAPTCHA to enhance their security.

KEYWORDS
CAPTCHAs, Interactive CAPTCHAs, Matching Task, Mouse Dynamics, Security

INTRODUCTION

CAPTCHAs have been extensively used to prevent robots from gaining automated access to online resources. According to analyst reports, Bots firmly took over the web in 2013 by contributing to 61.5% of web traffic, which comprises a 20% rise from 51% in 2012.¹ This is an alarming trend as 31% of this activity is attributed to malicious Bots.²

The ongoing developments in artificial intelligence make attack algorithms increasingly more sophisticated (Nguyen et al., 2012c; Cruz-Perez et al., 2012; Lin et al., 2011; Yan & El Ahmad, 2008; Beede, 2010; Nguyen et al., 2012b; Zhu et al., 2010; Bursztein, 2012; Nguyen et al., 2012a; Mori & Malik, 2003). The rising trend in Bot activity calls for the development of more secure mechanisms to inhibit their access to online resources. CAPTCHAs constitute an important line of defence against Bots. Many current CAPTCHAs rely on static images containing target objects or characters that users are expected to identify and type in. However, most such single-problem CAPTCHAs have been broken with high success rates. For example, reCAPTCHA has been recently broken with 99.8% accuracy (Goodfellow et al., 2013). One solution to the emerging threats to single-challenge CAPTCHAs is to convert them into dual-challenge CAPTCHAs by changing how solutions are submitted. Submitting CAPTCHA solutions requires human interaction and using intelligent human interaction would provide a natural extension to the original identification problem in single-challenge CAPTCHAs.

DOI: 10.4018/IJSSOE.2016010102

Copyright © 2016, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
Using the mouse as the means of interactivity provides ample opportunities to enhance CAPTCHA security, especially for CAPTCHAs that involve matching tasks.

In this paper, we develop several interactive matching tasks involving dynamic elements and demonstrate their impact on CAPTCHA security and usability through a series of tests and user studies. The proposed interactive tasks can be implemented in a myriad of other ways. However, our emphasis lies on the added level of security that can be achieved with simple provisions such as those proposed in this paper.

The proposed interactive tasks can be added to any existing CAPTCHA that has a matching task or can convert its solution task into a matching task. We apply these interactive tasks on a Unicode-based matching-task CAPTCHA, and measure its impact on this CAPTCHA’s security which shows substantial improvement. In addition, our user studies show that these matching tasks provide a straightforward and easy-to-solve challenge for human users while substantially complicating the process for machines. We also develop a profile of human users’ mouse movement patterns which can further help distinguish human users from Bots and enhance security. Our results provide a benchmark for future dual-challenge CAPTCHAs and offer readily implementable security enhancements to several types of existing single-challenge CAPTCHAs.

The remainder of this paper is structured as follows: we first provide an overview of CAPTCHAs with more focus on interactive CAPTCHAs, introduce a base CAPTCHA, and develop interaction-based challenges that will be added to the base CAPTCHA. Then, we assess the impact of these interactive challenges on the security and usability of the base CAPTCHA. We also explore how a profile of human mouse movement patterns can be used to enhance CAPTCHA security. Finally, we conclude the paper with a discussion of our findings and their implications for CAPTCHA design.

RELATED WORK

As a security mechanism against malicious programs that may use online resources, different types of CAPTCHAs have been developed. Most primary CAPTCHAs include one problem that users need to solve to show that they are human. The problem is usually a distorted image of a sequence of characters that a user needs to recognize (e.g. Von Ahn et al. 2008; Rusu et al., 2010), an image about which the user is asked questions (e.g. Ross et al., 2010; Banday & Shah, 2009), or a distorted audio clip whose contents should be detected by the user (Shirali-Shahreza et al. 2009).

In comparison with these single-problem CAPTCHAs, multi-problem CAPTCHAs have been designed to increase security against robot attacks by requiring the user to solve more than a single challenge. For example, Longe et al. (2009) proposed a 2-step CAPTCHA that contains a mathematical test (distinguishing numbers among alphanumeric characters and adding them together) and an image test. Another example is IMAGINATION proposed by Datta and Wang (2005), which consists of two steps of image selection and image annotation.

Another strategy that CAPTCHA designers have used to improve the security of CAPTCHAs is using mouse actions, such as clicking or drag and drop tasks, which are hard to emulate for computer programs. Examples of such CAPTCHAs include 3D CAPTCHA (Rolko, 2010) and 3D drag-n-drop CAPTCHA (Chaudhari et al., 2011). In 3D CAPTCHA, the user needs to use the mouse to rotate a 3D model and find the correct position of rotation. 3D Drag-n-Drop CAPTCHA asks users to drag and drop a rotated version of the displayed Latin characters to their respective locations in the sequence. We provide more examples of this type of CAPTCHAs, which we call interactive CAPTCHAs, in the next section.

In this paper, we propose a new two-challenge interactive CAPTCHA that has advantages over existing two-challenge CAPTCHAs and interactive CAPTCHAs. While users solve two different tests in existing two-challenge CAPTCHAs, the second challenge in our proposed CAPTCHA is embedded in the answer-submission process and is not viewed as a second challenge by users; however, robots still need to solve two different problems to be able to break the CAPTCHA. In terms of interactivity,
Examining the Quality of Evaluation Frameworks and Metamodeling Paradigms of Information Systems Development Methodologies
www.igi-global.com/chapter/examining-quality-evaluation-frameworks-metamodeling/23795?camid=4v1a

Software Engineering and HCI
www.igi-global.com/chapter/software-engineering-hci/29385?camid=4v1a

ART-Improving Execution Time for Flash Applications
Ming Ying and James Miller (2011). International Journal of Systems and Service-Oriented Engineering (pp. 1-20).
www.igi-global.com/article/art-improving-execution-time-flash/55059?camid=4v1a