Chapter 10
Secure Human-Computer Interaction: A Multi-Factor Authentication CAPTCHA Scheme

Emmanuel Oluwatobi Asani
https://orcid.org/0000-0002-6774-8529
Landmark University, Nigeria

Anthony Jatau Balla
Landmark University, Nigeria

Olumide Babatope Longe
American University of Nigeria, Nigeria

Roseline Oluwaseun Ogundokun
https://orcid.org/0000-0002-2592-2824
Landmark University, Nigeria

Emmanuel Abidemi Adeniyi
Landmark University, Nigeria

ABSTRACT

In this chapter, CAPTCHA was presented as a measure for secure human-computer interaction. A multi-factor CAPTCHA scheme that integrates facial recognition and real-time functionality as a secure verification mechanism to check the activities of bots that try to assume human status was designed, developed, and tested. The real-time functionality is premised on the human user's ability to complete trivial tasks which though simple for human is difficult to break by bots. This was motivated by the need to combat attackers' tendencies to beat existing CAPTCHA schemes through optical character recognition, image annotation, tag classifier, etc. Literature on a number of existing schemes was reviewed with a view to identifying gaps and establishing the research agenda. The system design and analysis were done using scalable design techniques. Implementation was done using Javascript and a set of APIs. The scheme was tested on an intel core i7 3GHz computer and further evaluated. Preliminary results and findings show a promising effectiveness and efficiency of the developed system.

DOI: 10.4018/978-1-7998-1279-1.ch010

INTRODUCTION

Human-Computer Interaction (HCI), also known as Human-Machine Interaction bothers on the study, design, development, and deployment of interactive systems and how humans relate with them, especially with a focus on functionality and usability (Jain and Sivaselvan, 2012). Thus, HCI considers activities and services offered by a system and how users can derive the maximum benefits accrued, to achieve specified goals in terms of ease of use and remembrance of how to use it, learnability, efficiency, error management and satisfiability (Brodić and Amelio, 2017).

Owing to its continued advances, ubiquity, and vast potentials, the internet has become a platform for the design, development, and deployment of Human-Computer Interactive (HCI) systems. Thus, there is an increasing need and demand for web-based HCI systems (Khalil, 2018). Consequently, HCI systems are susceptible to security issues plaguing internet technology and applications. This may explain the research interests in HCI security.

HCI security (HCI-Sec) studies the interaction between humans and machines as it relates to information security (Agathonos, 2016). Since, web-related resources are susceptible to security challenges such as Denial of Service, identity theft, phishing, XPath injection attacks and so on (Chaudhary *et al.,* 2015; Ajayi *et al.,* 2016; Jambhekar *et al.,* 2016; Omotosho *et al,* 2019), the aim of HCI-Sec, is to improve the security of information in HCI, while not compromising the usability of end-user applications (Garfinkel and Lipford, 2014; Asani *et al*., 2018). HCI-Sec considers aspects of user authentication, e-mail security, device pairing, anti-phishing schemes, web privacy, mobile security among others (Lampson, 2009; Kainda et al., 2010; Weir et al., 2010; Larrocha *et al.,* 2011; Garfinkel and Lipford, 2014; Kanakaris *et al.,* 2019).

In this chapter, CAPTCHA is presented as an authentication scheme for secure Human-Machine Interaction. The study aims to present a multi-factor authentication captcha scheme based on facial authentication and human ability to complete trivial tasks. The objectives of the study are to develop a real-time CAPTCHA system, to embed a Facial authentication system for secondary authentication and finally to develop an integrated multi-factor authentication system.

BACKGROUND

HCI-Sec centers around the user's need for usable and secure computers (Satchell and Dourish, 2009; González-Pérez *et al.,* 2019). The objective is to prevent criminals or illegitimate users from gaining unauthorized access or compromising the system's security without compromising the system's usability. Thus, techniques for securing the systems must encompass elements of usability, because perceived difficulties often result in users resorting to practices that circumvent security or alternatively, users may seek easier to use, but insecure systems (Smith 2003; Kainda *et al.,* 2010). Faily and Fléchais, (2010) noted that users' biases and perception play a prominent role in the balancing of security and usability. Thus, they proposed the IRIS framework with an underlying model that integrates usability, requirements, and risk analysis. Osho *et al.,* (2019), highlighted the increasing demand for secure systems, without compromising effectiveness engendered by usability, convenience, and cost-effectiveness.

Kamoun and Halaweh (2012) conducted an empirical study on 247 subjects to investigate the relationship between interface design and how the system's security is perceived. Their work was based on the hypothesis that effective interface design would positively affect the perception of the security of

Neuromarketing from the Perspective of Advertising Professionals: A Battle between Creatives and Strategic Planners

Ugur Bakir, Muge Elden and Erdem Gecit (2017). *Applying Neuroscience to Business Practice (pp. 257-276).*

www.igi-global.com/chapter/neuromarketing-from-the-perspective-of-advertising-professionals/170269?camid=4v1a