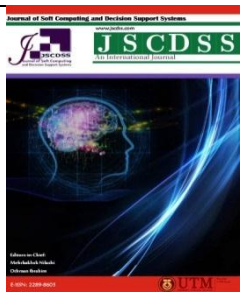
An International Journal
JSCDSS
http://www.jscdss.com
Vol.4 No.1 February 2017: 19-25
Article history:
Accepted 20 February 2017
Published online 25 March 2017

Journal of Soft Computing and Decision Support Systems



E-ISSN: 2289-8603

A Novel Two-Factor Authentication System Robust Against Shoulder Surfing

Mohammadreza Hazhirpasand Barkadehi [a,*], Mehrbakhsh Nilashi [a], Othman Ibrahim [a]
[a] Faculty of Computing, Universiti Technologi Malaysia, Johor, Malaysia

*** Corresponding author email address**: mhhazhirpasand@gmail.com

Abstract

To stop attackers from accessing protected contents of a website or a mobile application, authentication systems with various forms are presented. One of the challenging barriers in nowadays identification systems is unauthorized bystanders. This attack is mostly applicable on many sorts of authentication systems. To fight with unauthorized eyes, many approaches have been proposed. Each one has its own pros and cons. In this paper, the proposed system is a two-factor authentication in conjunction of smart-phone of owner. To disable malicious softwares to key log keystrokes or take screenshot or observers to memorize your hand movement on keyboard or mouse curse on a virtual keyboard, proposed system came up with a novel way to decrease the effect of these attacks.

Keywords: User authentication, Two-step authentication, Shoulder surfing attack

1. Introduction

Authentication systems have been changing through the passage of time. At first, password-based authentications were popular because of its simplicity of remembrance and applicability among people (Shen et al., 2016). Due to the fact of simplicity, valuable pieces of information or assets are protected by simple passwords and this causes insecurity for data owners. The essence of a password is exposed to many easy-to-run attacks such as phishing, social engineering or keylogging technique (Svogor and Kisasondi, 2012). Each of password characteristics such as password length, password composition and password selection reveals different concern which some designers take some or all of them into consideration to force users to choose a strong password (Shen et al., 2016). As a result, authentication systems gradually became more creative. For instance, on-the-fly password policy systems indicate weakness or strength of user chosen password according to the password characteristics as mentioned before.

Later graphical passwords introduced to boost the security strength of systems but still they were vulnerable to shoulder surfing and recording attacks (Prabhu & Shah, 2015). With the advent of new paths in related technologies, mixing password-based systems with other factors such as biometric or ownership increased the assurance of data safety to some extent. Biometric factor has two sub-categories of biometric authentication, physiological and behavioural (Kang et al., 2014). As physiological authentication name implies, it is regarded as measurement and recognition of physical specifications such as fingerprint, iris recognition and on the other hand, behavioural authentication relies on behavioural characteristics of the person such as keystroke dynamics (Bailey, 2014). Physiological examples such as fingerprints are sensitive to spoofing techniques, however, behavioural biometrics are much more suitable for second phase of authentication and need less additional hardware (Chen et al., 2015). Two-factor authentication systems nowadays mostly use a smartphone in industrial scales such as Yahoo or Google because of their availability in our any day-to-day life (Crossman and Liu, 2016; Abdurrahman et al., 2013).

In this study, a two-factor authentication model comprised of a traditional password and a virtual keyboard are presented. The second factor involves a smartphone to cooperate in order to accomplish the process of identification. Often on-screen keyboards are vulnerable to observers and software which are capable of taking screenshot stealthy. The considerable part of this system is neither a real user nor observers can see the on-screen keyboard.

2. Literature review

Current stage of research in this area contains different novel ideas to battle with onlookers and malicious software. As a result, different ideas on different devices and platforms have been implemented so far. For example, Shankar et al. (2016) proposed a system called IPCT which improves mobile authentication systems. In their system, a user must select a series of pictures and for enhancing security aspect, the amount of time that user holds the image button and tapping of fingers on the screen will be