International Journal of Digital Crime and Forensics
Volume 9 • Issue 1 • January-March 2017

Age Detection Through Keystroke Dynamics from User Authentication Failures

Ioannis Tsimperidis, Democritus University of Thrace, Komotini, Greece
Shahin Rostami, Bournemouth University, Poole, UK
Vasilios Katos, Bournemouth University, Poole, UK

ABSTRACT

In this paper an incident response approach is proposed for handling detections of authentication failures in systems that employ dynamic biometric authentication and more specifically keystroke user recognition. The main component of the approach is a multi layer perceptron focusing on the age classification of a user. Empirical findings show that the classifier can detect the age of the subject with a probability that is far from the uniform random distribution, making the proposed method suitable for providing supporting yet circumstantial evidence during e-discovery.

KEYWORDS

Age Classifier, Age Detection, Biometrics, Multi Layer Perceptron, Offender Profiling

INTRODUCTION

In today's modern digital communications, user authentication failures may lead to a series of incidents where if a user's identity is misrepresented, it could cause, among other issues, false accusations, leading to misconduct of justice. In its simplest form, consider a scenario of an unattended laptop where an adversary sends an insulting email by spoofing the legitimate owner. If traditional forensics are used, the laptop could be identified, seized and analysed to prove that the particular device was the email's origin. However, in digital forensics it is of utmost importance to "put fingers on keyboard", that is, to identify the physical person that performed the action. Another scenario relates to systems that offer seamless, continuous, and transparent biometric authentication (Flior and Kazimierz, 2010). In a typical setting, once authentication fails, the user – hopefully the perpetrator and not the legitimate user, as can happen in many cases due to the Type I errors such authentication systems exhibit – would be denied access. In our proposal, if user authentication fails at some point in time, the system should have the ability to record the user's typing behaviour in order to gather his/her characteristics such as gender, handedness, age, and so forth. As this is acknowledged to be a challenging problem (Uludag et al., 2004) with relatively poor success rates, we consider the use of epistemic uncertainty handling frameworks (Katos and Bednar, 2008). More specifically, in this paper we propose a system that is based on keystroke duration measurements in order to provide circumstantial evidence for supporting a forensic analyst to make an informed judgement on the identification of a suspect. Clearly, as it is very common in forensic science practice, the information gathered from the proposed system would need to be correlated with other sources (such as GSM geolocation data (Lessard and Kessler, 2010), security cameras, as well as physical evidence if applicable), in order to allow further reduction of the

DOI: 10.4018/IJDCF.2017010101

uncertainty surrounding the crime scene. Accepting that the evidence is circumstantial, we can relax the requirements of high success rates, but nevertheless, it is expected that the proposed solution will provide results that will be significantly diverging from a uniform distribution. The main contribution and novelty of this paper is on the application of neural networks for improving forensic readiness by providing indication and circumstantial evidence on an author's age. An age detection component has a number of applications, both as a proactive security measure (e.g. alerting a minor in the case they believe they are chatting on a social networking site with a young person whereas they may be chatting with a potential predator), following thus the security by design approach, as well as a post mortem tool for performing attribution on a potentially offensive content.

The rest of the paper is organized as follows. A survey of the literature is presented followed by the description of the data acquisition method and approach to parameter extraction required to perform keystroke dynamics. The paper continues by developing the classifier employed in the proposed method and the empirical evaluation.

RELATED WORK

Artificial Neural networks were used in the past to classify computer users or computer items into some categories. For instance, Clark et al. (2003) presented an artificial neural network based system for automated e-mail filing into folders and anti-spam filtering. Nogueira et al (2005) and Auld et al (2007) dealt with Internet traffic. More specifically, Noguiera et al. (2005) proposed the classification of Internet users into groups according to their average transfer rate. Auld et al. (2007) classified flows based on header-derived statistics, and this is feasible even when the IP (host) address and application port number are not known.

A number of diverse approaches on artificial neural networks for age classification exist in the literature. Hewahi et al. (2010) for instance proposed neural network classifiers to determine the age using image analysis techniques. They examined 4 age classes, each of them divided into two subcategories, used 68 landmark points taken from face images and achieved a success rate of 78.4%. Similarly, Choobeh (2012) used the same number of landmark points, applied 130 attributes to each of the artificial neural network classifiers that involved and calculated the mean absolute error of exact age between 4.85 and 5.85 years. Yi et al (2014) reduced the mean absolute error further to 3.63 years, which is an acceptable value to supply a more stable age estimator for practical applications.

Determining a blog's author age group is another perspective in this field. Schler et al. (2006) divided users into three age classes and based on the authoring style, but also the content of the blogs, achieved a classification success rate of about 76%. Rangel et al (2013) presented the results of the first International Author Profiling Task in which, researchers examined blogs written in two different languages: English and Spanish. Several different features were selected and the best approach achieved a classification accuracy of 64%.

The wide expansion of social networks has motivated the researchers to develop techniques for determining a user's attributes when these are not disclosed on their personal profile. Rao et al (2010) proposed an approach to automatically discover a number of user attributes by examining their status messages, the social network structure and communication behaviour of the users. They created a data set from 2000 users, who were divided into two classes, users who are under 30 and users who are over 30, used a Support Vector Machine, SVM, classifier and attained a classification accuracy rate of about 74%. The work by Pennacchiotti and Popescu (2011) and Bergsma et al. (2013), also dealt with social networks. In this case parameters like linguistic content and contacts between users were considered and used to predict ethnicity, political affiliation and origin.

This paper builds upon the concept of user classification using keystroke dynamics. The underpinnings of the proposed approach have roots to the Halstead-Reitan Battery, which is a sequence of neuropsychological tests that include a finger-tapping test (Strauss et al., 2006). This test measures the rate at which a subject repeatedly pushes a button. Empirical results show correlation