Behavioral Biometrics:
Categorization and Review

Roman V. Yampolskiy, University of Louisville, Louisville, KY, USA

Nawaf Ali, University of Louisville, Louisville, KY, USA

Darryl D'Souza, University of Louisville, Louisville, KY, USA

Abdallah A. Mohamed, University of Louisville, Louisville, KY, USA

ABSTRACT

This work categorizes and reviews behavioral biometrics with the inclusion of future-oriented techniques. A general introduction to this field is given alongside the benefits of this non-intrusive approach. It presents the examination and analysis of the current research in the field and the different types of behavior-centric features. Accuracy rates for verifying users with different behavioral biometric approaches are compared. Privacy issues that will or may arise in the future with behavioral biometrics are also addressed. Finally, the general properties of behavior, the influence of environmental factors on observed behavior and the potential directions for future research in the field of behavioral biometrics are discussed.

Keywords: *Authorship, Behavioral Biometrics, Features, Human Computer Interaction, Motor-Skill, Privacy, Taxonomy, User Verification*

1. INTRODUCTION TO BEHAVIORAL BIOMETRICS

With the proliferation of computers in our everyday lives need for reliable computer security steadily increases. Biometric technologies provide user friendly and reliable control methodology for access to computer systems, networks and workplaces (Angle, Bhagtani, & Chheda, 2005; Dugelay et al., 2002; K. Lee & Park, 2003). The majority of research is aimed at studying well established physical biometrics such as fingerprint (Cappelli, Maio, Maltoni, Wayman, & Jain, 2006) or iris scans (Anil K. Jain, Ross, & Prabhakar, 2004). Behavioral biometrics systems are usually less established, and only those which are in large part based on muscle control such as keystrokes, gait or signature are well analysed (Bolle, Connell, Pankanti, Ratha, & Senior, 2003; Delac & Grgic, 2004; Anil K Jain, Pankanti, Prabhakar, Hong, & Ross, 2004; Ruggles, 2007; Solayappan & Latifi, 2006; Uludag, Pankanti, Prabhakar, & Jain, 2004).

Behavioral biometrics provide a number of advantages over traditional biometric technologies. They can be collected non-obtrusively or even without the knowledge of the user.

DOI: 10.4018/ijncr.2014070105

Collection of behavioral data often does not require any special hardware and is so very cost effective. While most behavioral biometrics are not unique enough to provide reliable human identification they have been shown to provide sufficiently high accuracy identity verification. This paper is based on "Behavioral Biometrics: a Survey and Classification." by R. Yampolskiy and V. Govindaraju, which appeared in the International Journal of Biometrics, 1(2008), 81-113. The paper presents a new comprehensive overview and improvements on research previously published in a number of publications including (Yampolskiy, 2006, 2007a, 2007b, 2007c, 2007d, 2008a, 2008b; Yampolskiy & Govindaraju, 2006a, 2006b, 2007a, 2007b, 2008).

One of the defining characteristics of a behavioral biometric is the incorporation of time dimension as a part of the behavioral signature. The measured behaviour has a beginning, duration, and an end (Bioprivacy.org, 2005a). Behavioral biometrics researchers attempt to quantify behavioral traits exhibited by users and use resulting feature profiles to successfully verify identity (Bromme, 2003).

Behavioral biometrics can be classified into five categories based on the type of information about the user being collected. Category one is made up of authorship-based biometrics, which are based on examining a piece of text or a drawing produced by a person.

Category two consists of Human Computer Interaction (HCI) based biometrics (Yampolskiy, 2007a). In their everyday interaction with computers human beings employ different strategies, use different style and apply unique abilities and knowledge. Researchers attempt to quantify such traits and use resulting feature profiles to successfully verify identity. HCI-based biometrics can be further subdivided into additional categories, first one consisting of human interaction with input devices such as keyboards, computer mice, and haptics which can register inherent, distinctive and consistent muscle actions (Bioprivacy.org, 2005b). The second group consists of HCI-based behavioral biometrics which measure advanced human behaviour such as strategy, knowledge or skill exhibited by the user during interaction with different software.

Third and probably the best researched group of behavioral biometrics relies on motor-skills of the users to accomplish verification (Yampolskiy, 2007c). Motor-skill is an ability of a human being to utilize muscles. Muscle movements rely upon the proper functioning of the brain, skeleton, joints, and nervous system and so motor skills indirectly reflect the quality of functioning of such systems, making person verification possible. Authors adopt definition for motor-skill based behavioral biometrics, a.k.a. *kinetics,* as those biometrics which are based on innate, unique and stable muscle actions of the user while performing a particular task (Caslon.com.au, 2005).

Fourth and final category consists of purely behavioral biometrics. Purely behavioral biometrics are those which measure human behaviour directly not concentrating on measurements of body parts or intrinsic, inimitable and lasting muscle actions such as the way an individual walks, types or even grips a tool (Caslon.com.au, 2005). Human beings utilize different strategies, skills and knowledge during performance of mentally demanding tasks. Purely behavioral biometrics quantifies such behavioral traits and make successful identity verification a possibility.

All of the behavioral biometrics reviewed in this chapter share a number of characteristics and so can be analysed as a group using seven properties of good biometrics presented by Jain et al. (A. K. Jain, Bolle, & Pankanti, 1999; Anil K. Jain et al., 2004):

- **Universality:** Behavioral biometrics are dependent on specific abilities possessed by different people to a different degree or not at all and so in a general population universality of behavioral biometrics is very low. But since behavioral biometrics