Chapter 1
Taxonomy of Behavioural Biometrics

Roman V. Yampolskiy
University of Louisville, USA

Venu Govindaraju
University at Buffalo, USA

ABSTRACT

This chapter presents a taxonomy of the latest behavioural biometrics, including some future oriented approaches. Current research in the field is examined and analyzed along with the features used to describe different types of behaviour. After comparing accuracy rates for verification of users using different behavioural biometric approaches, researchers address privacy issues which arise or might arise in the future with the use of behavioural biometrics. Finally, generalized properties of behaviour are addressed as well as influence of environmental factors on observed behaviour and potential directions for future research in behavioural biometrics.

INTRODUCTION TO BEHAVIORAL BIOMETRICS

With the proliferation of computers in our every day 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; 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 (Jain, Ross, & Prabhakar, 2004d). Behavioural 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 analyzed (Bolle, Connell, Pankanti, Ratha, & Senior, 2003; Delac & Grgic, 2004; Jain, Pankanti, Prabhakar, Hong, & Ross, 2004c; Ruggles, 2007; Solayappan & Latifi, 2006; Uludag, Pankanti, Prabhakar, & Jain, 2004).

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

DOI: 10.4018/978-1-60566-725-6.ch001

behavioural data often does not require any special hardware and is so very cost effective. While most behavioural biometrics are not unique enough to provide reliable human identification they have been shown to provide sufficiently high accuracy identity verification. This chapter is based on "Behavioral Biometrics: a Survey and Classification." by R. Yampolskiy and V. Govindaraju, which appeared in the International Journal of Biometrics, 1(1), 81-113. The chapter 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)

In accomplishing their everyday tasks human beings employ different strategies, use different styles and apply unique skills and knowledge. One of the defining characteristics of a behavioural biometric is the incorporation of time dimension as a part of the behavioural signature. The measured behaviour has a beginning, duration, and an end (Bioprivacy.org, 2005a). Behavioural biometrics researchers attempt to quantify behavioural traits exhibited by users and use resulting feature profiles to successfully verify identity (Bromme, 2003). In this section authors present an overview of most established behavioural biometrics.

Behavioural 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. Verification is accomplished by observing style peculiarities typical to the author of the work being examined, such as the used vocabulary, punctuation or brush strokes.

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 behavioural biometrics which measure advanced human behaviour such as strategy, knowledge or skill exhibited by the user during interaction with different software.

Third group is closely related to the second one and is the set of the indirect HCI-based biometrics which are the events that can be obtained by monitoring user's HCI behaviours indirectly via observable low-level actions of computer software (Yampolskiy, 2007b). Those include system call traces (Denning, 1987), audit logs (Ilgun, Kemmerer, & Porras, 1995), program execution traces (Ghosh, Schwartzbard, & Schatz, 1999a), registry access (Apap, Honig, Hershkop, Eskin, & Stolfo, 2002), storage activity (Pennington, et al., 2002), call-stack data analysis (Feng, Kolesnikov, Fogla, Lee, & Gong, 2003b) and system calls (Garg, Rahalkar, Upadhyaya, & Kwiat, 2006 ; Pusara & Brodley, 2004). Such low-level events are produced unintentionally by the user during interaction with different software.

Same HCI-based biometrics are sometimes known to different researchers under different names. IDS based on system calls or audit logs are often classified as utilizing program execution traces and those based on call-stack data as based on system calls. The confusion is probably related to the fact that a lot of interdependency exists between different indirect behavioural biometrics and they are frequently used in combinations to improve accuracy of the system being developed. For example system calls and program counter data may be combined in the same behavioural signature or audit logs may contain information about system calls. Also one can't forget that a human being is indirectly behind each one of those