Chapter 10

Mouse Dynamics
Biometric Technology

Ahmed Awad E. Ahmed
University of Victoria, Canada

Issa Traore
University of Victoria, Canada

ABSTRACT

In this chapter the Authors introduce the concepts behind the mouse dynamics biometric technology, present a generic architecture of the detector used to collect and process mouse dynamics, and study the various factors used to build the user’s signature. The Authors will also provide an updated survey on the researches and industrial implementations related to the technology, and study possible applications in computer security.

INTRODUCTION

Different types of biometrics are currently available in the market, and are widely used in various security applications. Biometrics can be classified into two categories, “physiological biometrics” and “behavioral biometrics”. Physiological biometrics identify the user based on physiological characteristics, such as fingerprints and eye retina/iris scanning, whereas behavioral biometrics depend on detecting the behavioral features of the user, such as signature, voice, and keystroke dynamics.

The utilization of biometrics, however, has so far been limited to identity verification in authentication and access control systems. Hence important security applications such as intrusion detection systems have been left out of this technology. We have identified two primary reasons for that. First, most biometric systems require special hardware device for biometrics data collection, which restricts their use to only networks segments that provide them, making the systems irrelevant for a significant number of remote users, who operate out of these network segments. Second, most biometric systems require an active involvement of the user who is asked to provide some data sample that can be used to verify his identity. This excludes the possibility of passive monitoring, which is essential for intrusion detection. There is also number of secondary obstacles to the use of biometrics for intrusion
Mouse Dynamics Biometric Technology

detection such as whether the technology allows
dynamic monitoring, or real-time detection.

A popular biometric system, which escapes
some of these limitations, is keystroke dynamics
biometrics. Keystroke dynamics does not require
special hardware device for data collection (a
regular keyboard is enough), and under certain
circumstances can be used for dynamic monitor-
ing. The same applies for a newly introduced
biometric based on mouse dynamics.

Mouse dynamics is a behavioral biometric
which was introduced at the Information Secu-
rity and Object Technology (ISOT) research lab,
University of Victoria in 2003 (Ahmed & Traore,
2003). Mouse Dynamics can be described as the
characteristics of the actions received from the
mouse input device for a user, while interacting
with a graphical user interface. Mouse actions
include general mouse movement, drag and drop,
point and click, and silence (i.e. no movement).
The raw data collected for each mouse movement
consists of the distance, time, and angle. The
behavioral analysis process utilizes statistical
approaches to generate a number of factors from
the captured set of actions; these factors are used
to construct what is called a Mouse Dynamics
Signature (MDS), a unique set of values char-
acterizing the user’s behavior measured over a
period of time.

Some of the factors consist of calculating the
average speed against the traveled distance, or cal-
culating the average speed against the movement
direction. Another set of factors can be calculated
as a result of studying the histogram of collected
measurements (individually or combined) such
as the histogram of the types of actions or the
durations of the silence periods.

Mouse and keystroke dynamics biometrics
are two related technologies, which complement
each other. While a mouse is very important for
graphical user interface (GUI) –based applications, a keyboard is essential for command –line
based applications.

One of its key strengths compared to traditional
biometric technologies is that it allows dynamic
and passive user monitoring. As such it can be
used to track reliably and continuously legitimate
and illegitimate users throughout computing ses-
sions.

Mouse Dynamics biometric is appropriate for
user authentication (with some limitations). It can
be effectively used for dynamic authentication or
identity confirmation in cases where the actions
of an active user raise some suspicions. The tech-
nology is also suitable for continuous monitoring
applications such as detecting masqueraders in
intrusion detection, or establishing the identity of
perpetrators in digital forensics analysis.

In this chapter we will introduce the concepts
behind the mouse dynamics biometric technol-
yogy, present a generic architecture of the detector
used to collect and process mouse dynamics, and
study the various factors used to build the user’s
signature. We will also provide an updated survey
on the researches and industrial implementations
related to the technology, and study possible ap-
plications in computer security.

BACKGROUND

In contrast to other behavioral biometrics which
were widely studied in computer security, previ-
ous works on mouse dynamics have, so far, been
limited to user interface design improvement
(Chan et al., 2001; Oel et al., 2001; Whisenand
& Emurian, 1996). In particular, mouse move-
ment analysis has been the purpose of extensive
research works. Studies have been conducted to
establish the applicability of Fitts’ law in predict-
ing the duration of a movement to a target based
on the size of the target and the distance from
the starting point to the target (Whisenand
& Emurian, 1996). According to Fitts’ law, the mean
movement time for a movement with distance
A to a target with width W is defined as $MT = a$
15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product’s webpage: www.igi-global.com/chapter/mouse-dynamics-biometric-technology/36921?camid=4v1

This title is available in InfoSci-Books, InfoSci-Medical, Healthcare, and Life Sciences, Biometrics and Surveillance Technologies, Communications, Social Science, and Healthcare, InfoSci-Select, InfoSci-Select. Recommend this product to your librarian: www.igi-global.com/e-resources/library-recommendation/?id=1

Related Content

Learning with Privileged Information for Improved Target Classification

Face Recognition in Adverse Conditions: A Look at Achieved Advancements
Maria De Marsico and Michele Nappi (2014). Face Recognition in Adverse Conditions (pp. 388-413). www.igi-global.com/chapter/face-recognition-in-adverse-conditions/106993?camid=4v1a

Comparison of SEMG Derived Parameters and Blood Oxygen Saturation in Monitoring Neuromuscular Fatigue in Humans

Dataveillance in the Workplace: Privacy Threat or Market Imperative?