Chapter 14

Evaluation of Keystroke Dynamics Authentication Systems: Analysis of Physical and Touch Screen Keyboards

Moustafa Dafer
Rafik Hariri University, Lebanon

Mohamad El-Abed
Rafik Hariri University, Lebanon

ABSTRACT

Keystroke dynamics authentication systems have shown promising results to be used in e-commerce and banking applications. However, this modality suffers from several limitations decreasing their widespread of use in daily applications. This chapter addresses the evaluation of keystroke dynamics authentication systems. The chapter provides an evaluation framework to be used when designing and comparing such systems. It also provides an analysis study of the collected features using a physical and touch screen keyboards. This chapter is dedicated to researchers and engineers who need to quantify the usability of their developed keystroke dynamics systems.

INTRODUCTION

Keystroke dynamics authentication solution is considered as a promising means for either enhancing or replacing traditional authentication systems based on “what we know” such as a password and “what we own” such as a badge (Bergadano et al., 2002; Clarke & Furnell, 2006). It is receiving more and more attention due to the fact that the keystroke dynamic biometrics approach is economical and can be easily integrated into personal computers, ATMs, cellular phones, and other devices with minimal alteration and user intervention (El-Abed et al., 2011). Despite the obvious advantages of keystroke dynamics
systems, their utilization in modern systems does not match their potential. The main drawback is the uncertainty of the verification result. By contrast to password checking, the verification of biometric raw data is subject to errors represented by a similarity percentage (100% is never reached). Other drawbacks related to vulnerabilities and usability issues exist (ISO/IEC FCD 19792, 2008). Thus, in order to achieve said potential and become adopted in modern day industries, their quality must be precisely quantified. A reliable evaluation methodology is needed to shed light on the merits of the new biometric system.

The goal of this chapter is twofold: First, it provides the biometrics community with an evaluation methodology of keystroke dynamics authentication systems which may be used during the development and comparison of such systems. In addition, it presents an analysis and comparison study of the collected features between a physical and touch screen keyboards.

The outline of the chapter is defined as follows: we present first the general concepts of keystroke dynamics technology as well as its limitations. Second, we present the evaluation methodology of keystroke dynamics authentication systems which may be used during the design and development of such systems. Third, an analysis and comparison study of the collected features between a physical and touch screen keyboards is presented. Fourth, we present the emerging trends in the keystroke dynamics research field followed by a conclusion.

**KEYSTROKE DYNAMICS TECHNOLOGY**

**Keystroke Dynamics Information**

Keystroke dynamics technology is used to discriminate individuals based on their way of typing a text (such as a password). An ideal authentication system should respect the following properties:

- **Universality:** All individuals must be characterized by this information.
- **Uniqueness:** This information must be as dissimilar as possible for two different individuals.
- **Permanency:** It should be present during the whole life span of an individual.
- **Collectability:** It can be measured in an easy manner.
- **Acceptability:** It concerns the possibility of a real use by users.

Table 1 presents a comparison study of biometric modalities in terms of universality, uniqueness, permanency, collectability and acceptability. From this table, we can deduce that no biometric information satisfies simultaneously all these properties. As for keystroke dynamics, it provides a good performance. However, the users’ typing behavior changes with mood and time thus permanency is not guaranteed.

**The General Scheme of a Keystroke Dynamics Authentication System**

The keystroke dynamics authentication process is divided into three main functionalities:

- **Enrolment**