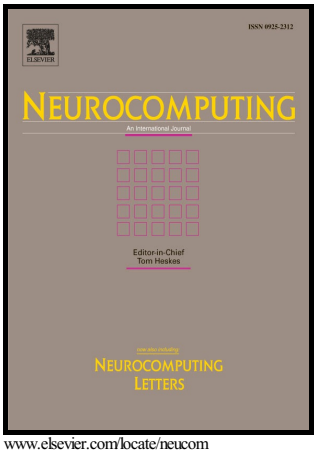

www.elsevier.com/locate/neucom

A study on Continuous Authentication using a combination of Keystroke and Mouse Biometrics

Soumik Mondal, Patrick Bours

PII: S0925-2312(16)31432-1
DOI: http://dx.doi.org/10.1016/j.neucom.2016.11.031
Reference: NEUCOM17787

To appear in: *Neurocomputing*

Received date: 23 November 2015
Revised date: 2 October 2016
Accepted date: 17 November 2016

Cite this article as: Soumik Mondal and Patrick Bours, A study on Continuous Authentication using a combination of Keystroke and Mouse Biometrics *Neurocomputing,* http://dx.doi.org/10.1016/j.neucom.2016.11.031

Available online at www.sciencedirect.com

ScienceDirect

NEUCOM

Neurocomputing 00 (2016) 1–44

A study on Continuous Authentication using a combination of Keystroke and Mouse Biometrics

Soumik Mondal and Patrick Bours

NISlab - Norwegian Information Security laboratory
NTNU - Norwegian University of Science and Technology
Gjøvik, Norway

soumik.mondal@ntnu.no, patrick.bours@ntnu.no

Abstract

In this paper we focus on a context independent continuous authentication system that reacts on every separate action performed by a user. We contribute with a robust dynamic trust model algorithm that can be applied to any continuous authentication system, irrespective of the biometric modality. We also contribute a novel performance reporting technique for continuous authentication. Our proposed approach was validated with extensive experiments with a unique behavioural biometric dataset. This dataset was collected under complete uncontrolled condition from 53 users by using our data collection software. We considered both keystroke and mouse usage behaviour patterns to prevent a situation where an attacker avoids detection by restricting to one input device because the system only checks the other input device. During our research, we developed a feature selection technique that could be applied to other pattern recognition problems.

The best result obtained in this research is that 50 out of 53 genuine users are never inadvertently locked out by the system, while the remaining 3 genuine users (*i.e.* 5.7%) are sometimes locked out, on average after 2265 actions. Furthermore, there are only 3 out of 2756 impostors not been detected, *i.e.* only 0.1% of the impostors go undetected. Impostors are detected on average after 252 actions.

Keywords: Continuous Authentication, Behavioural Biometrics, Mouse Dynamics, Keystroke Dynamics, Trust Model, Feature Selection, Performance Measure

1. Introduction

For most existing computer systems, once the user's identity is verified at login (referred to as Static Authentication (SA)), the system resources are available to that user until he/she exits the system or locks the session. In fact, the system resources are available to any user during that period. This may be appropriate for low security environments, but can lead to session hijacking, in which an attacker targets an open session, *e.g.* when people leave the computer unattended for shorter or longer periods when it is unlocked, for example to get a cup of coffee, to go and talk to a colleague, or simply because they do not have the habit of locking a computer because of the inconvenience. In