Informatics Institute of Technology

In Collaboration with

University of Westminster, UK

KeyAuth - Keystroke Dynamics based Continuous User Authentication as a Service

A dissertation by

Janak Amarasena (2014025)

Supervised By

Mr. Saman Hettiarachchi

Submitted in partial fulfilment of the requirements for the

BEng (Hons) Software Engineering degree

Department of Computing

Abstract

With the cybercrime rate at high levels, the need for a tightening of security in user accounts is growing. Currently, users are only authenticated at the entry point to the system and users only use single-factor authentication on most accounts which makes the accounts even more vulnerable. Attackers are even capable of hijacking already authenticated accounts. In order to defend against this, there should be a mechanism to continuously authenticate users without giving an overhead to the user experience. The author proposes a continuous authentication mechanism for secondary authentication based on keystroke dynamics. As it uses personalised data to authenticate a user it is more tamper-proof that other methods and also this method will not add any unwanted overhead to the user experience as it will be running on the background and will have a better user experience that existing secondary authentication mechanism. The author introduces a new classification algorithm based on the nearest neighbour algorithm and a new feature vector that can be used in a multi-device type environment (i.e. desktop, mobile and etc). A false acceptance rate 0.12 and a false rejection rate of 0.16 has been achieved by the systems' classification algorithm. These results were achieved by using only 200 keystrokes for initial training and 100 keystrokes for authentication. The system also includes a way to continuous update of user behavioural data which helps to improve the accuracy. The system uses a centralized service type deployment so multiple applications can make use of the service.

Subject Descriptors:

- Security and privacy ~ Security services ~ Authentication ~ Biometrics
- Security and privacy ~ Security services ~ Authentication ~ Multi-factor authentication
- Security and privacy ~ Human and societal aspects of security and privacy ~ Usability in security and privacy
- Theory of computation ~ Pattern matching
- Information systems ~ World Wide Web ~ Web services ~ RESTful web services

Key Words:

Multi-Factor Authentication, Continuous Authentication, Behavioural Biometrics, Keystroke Dynamics, Pattern Recognition, Continuous Update