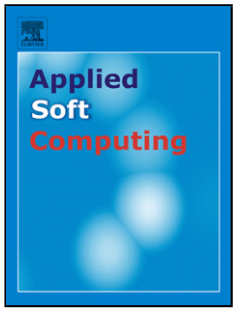
Accepted Manuscript



Title: Real-time Electrocardiogram Streams for Continuous Authentication

Author: Carmen Camara Pedro Peris-Lopez Lorena Gonzalez-Manzano Juan Tapiador

PII: S1568-4946(17)30443-X
DOI: http://dx.doi.org/doi:10.1016/j.asoc.2017.07.032
Reference: ASOC 4360

To appear in: *Applied Soft Computing*

Received date: 31-1-2017
Revised date: 7-7-2017
Accepted date: 13-7-2017

Please cite this article as: Carmen Camara, Pedro Peris-Lopez, Lorena Gonzalez-Manzano, Juan Tapiador, Real-time Electrocardiogram Streams for Continuous Authentication, *<![CDATA[Applied Soft Computing Journal]]>* (2017), http://dx.doi.org/10.1016/j.asoc.2017.07.032

Noname manuscript No.
(will be inserted by the editor)

Real-time Electrocardiogram Streams for Continuous Authentication

Carmen Camara · Pedro Peris-Lopez · Lorena Gonzalez-Manzano · Juan Tapiador

Received: date / Accepted: date

Abstract Security issues are becoming critical in modern smart systems. Particularly, ensuring that only legitimate users get access to them is essential. New access control systems must rely on Continuous Authentication (CA) to provide higher security level. To achive this, recent research has shown how biological signals, such as Electroencephalograms (EEGs) or Electrocardiograms (ECGs), can be useful for this purpose. In this paper we introduce a new CA scheme that, contrarily to previous works in this area, considers ECG signals as continuous data streams. The data stream paradigm is suitable for this scenario since algorithms tailored for data streams can cope with continuous data of a theoretical infinite length and with a certain variability. The proposed ECG-based CA system is intended for real-time applications and is able to offer an accuracy up to 96%, with an almost perfect system performance (kappa statistic $>$ 80%).

Keywords Datastreams · Healthcare · Identification · Electrocardiogram

1 Introduction

Security applications are gaining momentum in modern societies. With the advent of information technologies, data and resources are available almost anytime, anywhere. One key aspect is to ensure that the access to these elements is provided for authorized users only. This need is usually referred to as access control [1].

This work was supported by the MINECO grant TIN2013-46469-R (SPINY: Security and Privacy in the Internet of You); by the CAM grant S2013/ICE-3095 (CIBER- DINE: Cybersecurity, Data, and Risks), and by the MINECO grant TIN2016-79095-C2-2-R (SMOG-DEV - Security mechanisms for fog computing: advanced security for devices)

Carmen Camara, Lorena Gonzalez-Manzano, Juan Tapiador
Carlos III University of Madrid, Avda. de la Universidad 30, 28911, Leganes, Spain
Tel.: +34 91 6248877; Fax: +34 91 6249129
E-mail: macamara@pa.uc3m.es, {lgmanzan,jestevez}@inf.uc3m.es

Pedro Peris-Lopez
1. Carlos III University of Madrid, Avda. de la Universidad 30, 28911, Leganes, Spain
2. Aalto University, Konemiehentie 2, 02150 Espoo, Finland
E-mail: pperis@inf.uc3m.es or pedro.peris-lopez@aalto.fi