Use of Personal Rhythm to Authenticate Encrypted Messages

Authors : Carlos Gonzalez

Abstract : When communicating using private and secure keys, there is always the doubt as to the identity of the message creator. We introduce an algorithm that uses the personal typing rhythm (keystroke dynamics) of the message originator to increase the trust of the authenticity of the message originator by the message recipient. The methodology proposes the use of a Rhythm Certificate Authority (RCA) to validate rhythm information. An illustrative example of the communication between Bob and Alice and the RCA is included. An algorithm of how to communicate with the RCA is presented. This RCA can be an independent authority or an enhanced Certificate Authority like the one used in public key infrastructure (PKI).

Keywords : authentication, digital signature, keystroke dynamics, personal rhythm, public-key encryption
Conference Title : ICESSE 2017 : International Conference on Electronic Systems and Software Engineering
Conference Location : Istanbul, Türkiye
Conference Dates : September 28-29, 2017