

BIOGINA: An authentication software based on Keystroke Dynamics

Sylvain Hocquet^{1,2}, Jean-Yves Ramel², Hubert Cardot²

¹ Monecarte Rue Jean Monnet, 37160 DESCARTES - FRANCE

² Université François Rabelais de Tours, Laboratoire d'Informatique (EA 2101), 64 Avenue Jean Portalis, 37200 TOURS, France
{sylvain.hocquet, jean-yves.ramel, hubert.cardot }@univ-tours.fr

Abstract: Since a few years, the need of more security level for every day life has greatly increased. This kind of request has strongly accelerated the development of the biometric-based methods.

However, in most cases, these methods impose significant extra costs. In order to propose biometric methods of lower cost, we have studied the use of a device available on all the computers: the keyboard. Then, the authentication relies on the analysis of the way a user is typing on his keyboard: called Keystroke Dynamics.

The advantages of using keystroke dynamics compared to other biometric methods are:

- No additional hardware cost
- Good acceptance by users
- No more effort after enrolment for user compared to the traditional username

and password

Unfortunately, the disadvantage of the keystroke dynamics is weaker performances compared to other biometric methods based on physical features. That is why we have tried to improve such systems.

In our system, to extract data from the striking of a user, the times between keyboard events are used. A keyboard event can be the pressure or the release of a key.

To increase the performances, we propose different method to compute user-dependant parameters to control the keystroke dynamic system. These parameters include the security threshold and fusion weights of different classifiers. For more information on this works see [Hocquet, Ramel et al. 2006].

We have conducted several tests on a population of 42 users. The keystroke sequences were composed of user names and passwords of different lengths and impostors attacks for each user. Each user has provided between 20 and 110 logins sequences and has been attacked between 20 and 100 times. Obtained results show that keystroke dynamics can be used to perform authentication or identification in real case applications with an Equal Error Rate around 5%.

Our software is called BIOGINA, and can replace the Microsoft Graphical Identification and Authentication system (MSGINA) which is call at the start of Windows system. We replace the MSGINA function using to login in the system and to change password.

Our software adds an authentication of the keystroke dynamics of username and password. The lengths of this sequence must not be under eight characters. To enroll a user must strike 10 times the couple password and username.

Using this low cost software, we have a useful authentication device, which need only software installation, and provided a great improvement compared to the classical Windows authentication.

Hocquet, S., Ramel, J.-Y., et al. (2006). Estimation of User Specific Parameters in One-class Problems. 18th International Conference on Pattern Recognition, Hong Kong.