Efficiency Issues and Improving Implementation of Keystroke Biometric Systems

Ali Kartit
https://orcid.org/0000-0002-3472-1151
LTI Laboratory, ENSAJ, Chouaib Doukkali University, Morocco

Farida Jaha
LTI Laboratory, ENSAJ, Chouaib Doukkali University, Morocco

INTRODUCTION

Employees use more and more their mobile devices in work specifically after having introduced a new trend called BYOD (Bring Your Own Devices) that allows workers to provide their own devices and use the same materials for both personal and professional purposes. This new practice improves employee productivity by using of a mastered mobile device and it decreases the budget spent on IT because the materials used are purchased and maintained by employees at the same time it offers disadvantages like security issues. Therefore, it is very important to use an authentication platform like authentication based on knowledge (password, etc.), physical biometric authentication (iris, etc.) or behavioral biometric authentication (keystroke dynamics, etc.) to avoid data leakage.

This paper deals with biometric authentication based on keystroke dynamics. The method consists of analyzing the typing patterns of a claimed user and then decide to accept or reject the user authentication attempt.

The main advantages of keystroke dynamics are: (1) it improves productivity by using a known device, (2) As the user is typing his login and password; biometric data is extracted and compared to a reference profile stored in the system database without the need of an extra time to verify the user, (3) it allows a reduction in investment, it does not require external hardware. The keystroke dynamics implementation is based essentially on software, which is the subject of this paper.

keystroke can be integrated into several applications, whether web applications, behavioral intrusion detection system, online banking, etc. Its flexibility comes from the fact that the administrators of its systems do not have to force the user to buy additional equipment (e.g fingerprint capture, iris capture, voice capture, etc.) to read the end user's biometric data.

The paper sections are organized as follows: the first section is the methodology followed in the article where we presented the keystroke dynamics technique with its characteristics and the sensors used in the software (dwell time and digraph time). In the same section, we also mentioned some real-world application of this technique and finally the architecture adopted in the development of the software. The second section is the proposed work in which the four phases (registration, enrollment, authentication and classification) have been detailed. We then treated the setting part and the error metrics that we will use to test the accuracy of the software.

DOI: 10.4018/978-1-5225-9715-5.ch077

BACKGROUND

Keystroke dynamics was and remains a strong field for research, the first documented research published by Forsen, Nelson and Staron (1977) dated back to 1977. Later, many other papers were appeared. For instance, Patil and Renke (2016) published a paper where they better cleared up keystroke dynamics, they mentioned some drawback of this biometric method and they distinguished two different keystroke dynamics authentications: static and continuous. In static, the user is asked to type his login and password, then he is validated by comparing those data with his pre-calculated profile. In the continuous authentication, the end-user's biometric data is captured throughout the use of the system. The use of the second kind of authentication prevents an impostor from taking control of the machine when its legal user is absent (several users leave their workstations without locking them or putting them in sleep mode). In this case keystroke recognition can be used as a behavioral intrusion detection system. Grant Pannell and Helen Ashman (2010) combined a set of factors including CPU usage, sites visited and keystroke biometric to implement a behavioral IDS to detect unauthorized users through their system usage. On the same page, Avasthi and Sanwal (2016) gave the existing approaches, security and challenges of keystroke dynamics in order to motivate the researches to further come with more innovative improvements. Some other researchers like Panasiuk, Dabrowski, Saeed, and Bochenska-Wlostowska (2014) devoted their studies to compare different keystroke dynamics databases and to test if the same algorithm running on two theoretically identical databases gives the same results.

Other research tried to improve the EER (Error Equal Rate) and the security level of the devices using keystroke biometric like Morales, Falanga, Fierrez, Sansone, and OrtegaGarcia (2015) team and Nagargoje, Lomte, Auti, and Rokade (2014) team who combined keystroke and mouse movement to authenticate the user and increase the device confidentiality.

Systems with touchscreens, which are replacing more and more traditional computer systems, arouse researchers like Kambourakis, Damopoulos, Papamartzivanos, and Pavlidakis (2014). They try to adapt keystroke dynamics authentication to this kind of screen. Teh, Zhang, Teoh, and Chen (2016) gave us an overview and survey of a touch dynamics authentication system available for devices with touchscreen.

Morales, Fierrez and Tolosana (2016) focused on reporting the results of 31 different algorithms evaluated according to accuracy and robustness.

Liakat, Monaco, Tappert and Qiu (2017) presented a detailed survey of the most recent researches on keystroke dynamic authentication. They analyzed different methods, algorithms used, the accuracy rate, and the shortcomings of those investigations. In the same direction, Teh, Zhang, Teoh and Chen (2016) presented a survey of user authentication using keystroke dynamics.

Further, new studies are focused on analyzing keystroke recognition method for smartphones such as Ho's research published in 2014 and later Alzubaidi and Kalita in 2015, they highlight some problems that concern smartphones security in fact that smartphones are small in size and they can easily be lost or be stolen which increases the need to use two-factor authentication. Different research has shown that keystroke dynamics can be adapted to different systems. For example, Antal, Szabo, and Làszlo (2015) demonstrated experimentally, using Android devices, that touchscreen-based features improve keystroke dynamics based identification and verification. Boakye and Marfo (2016) determined the effectiveness of keystroke analysis and password security synergy to authenticate users of a system web-based applications. Another example to give is Babaeizadeh, Bakhtiari, and Maarof (2014) who address using keystroke authentication in mobile cloud computing.