

Keystroke Dynamics: Towards Realtime Keyboard Usage Monitoring

Abdullah Alshehri, Frans Coenen, Danushka Bollegala
Department of Computer Science, University of Liverpool, United Kingdom
{a.a.alshehri, coenen, danushka.bollegala}@liverpool.ac.uk

POSTER ABSTRACT

The diversity of keyboard dynamics (behaviour) means that it can be used to differentiate keyboard users from one another (Gaines et al. 1980). Consequently keyboard dynamics can be employed to monitor keyboard users to ensure that they are who they say they are. This is important with respect to a number of application domains such as online assessment and security monitoring. Keyboard dynamics in this context are measurable features such as: the length of time a key is held down, the time between individual key presses (flight time), temporal patterns associated with sequences of key presses, and so on. The advantage that keyboard dynamics has over other types of identification is that it can be employed to provide continuous monitoring and requires no additional equipment. Unlike physiological traits (such as fingerprint and iris recognition) where an imposter can replace the legitimate user after successful identification has been completed. The usage of keystroke dynamics is a promising mechanism for determining the authenticity of computer users. There has been little reported work on keystroke dynamics for continuous user authentication; some authors have suggested that it is unreliable as an authentication tool (Ahmed & Traore 2014). However, it is argued here that this claimed unreliability is a feature of the small number of mechanisms that have been considered to date, not the concept of continuous user authentication using keyboard dynamics itself.

The work described here considers the concept of keystroke dynamics from a time series analysis point of view making use of the observation that keystrokes occur as discrete time events. The idea is that we can continuously monitor users, the monitoring may not be correct at all time points but as the process progresses the weighting of the evidence will increase (positively or negatively). Other than the learning process to be adopted the work features a number of additional challenges as follows: (i) the text to be monitored is not predefined (unlike in the case of, for example, passwords), (ii) the high dimensionality of the features to be considered (for example key stroke pairs and triples), and (iii) the effect that the diversity of keyboard layout has on keyboard dynamics. However, it is suggested that by addressing these issues, coupled with the usage of superior learning algorithms and techniques than those considered to date, keyboard dynamics can be successfully used to monitor keyboard usage.

To investigate our perspective the work was focussed on an e-learning domain

where we wished to authenticate student identities. We developed a web-based interface to mimic the Blackboard system (a well know e-learning system), and asked a number of students to answer three general questions. The system had a Web-Based Keystroke Timestamp Recorder (WBKTR) tool operating in the background so as to record the timestamp for each stroke. Students were asked to write at least 100 words in response to each question with no maximum limitation; 100 words was considered sufficient to allow for identification (Gunetti & Picardi 2005). Thus for each keystroke, k_i , three timing values were collected (key-up, key-down and key hold) plus a categorical value (ASCII value). We selected N samples and divided each sample into two to give two sets, s_1 and s_2 , a training set and a test set. We represented each set as a collection of time series. Evaluation was conducted by measured the similarity between each training sample and each test sample, the idea being to see if we could identify the correct test sample. The comparison was conducted using a method known as Dynamic Time Wrapping (DTW). This gives a similarity measure, known as the Warping Distance (WD). The lower the WD with respect to two time series the similar the two time series are. The recorded results show that out of 162 comparisons there were 12 false positives (alternative users accepted as the real user). The global evaluation metric used was Mean Reciprocal Rank (MRR), we obtained an MRR of 0.637, a clear indicator that the technique has significant potential and merits further investigation.

References

- Ahmed, A. A. & Traore, I. (2014), 'Biometric recognition based on free-text keystroke dynamics', *Cybernetics, IEEE Transactions on* **44**(4), 458–472.
- Gaines, R. S., Lisowski, W., Press, S. J. & Shapiro, N. (1980), Authentication by keystroke timing: Some preliminary results, Technical report, DTIC Document.
- Gunetti, D. & Picardi, C. (2005), 'Keystroke analysis of free text', *ACM Transactions on Information and System Security (TISSEC)* **8**(3), 312–347.