Detection of Cheating Students by Implicit Verification of Identity in eLearning systems

Peter Krátky

Abstract: *Dishonest behaviour of students in e-learning systems could be suppressed by an additional implicit verification of a user's identity. The method proposed in this paper detects presence of illegitimate user according to computer mouse usage characteristics. We present performance results of the method evaluated in an e-learning system. Further, we experimented with predicting Index of Learning Styles based on the mouse characteristics in order to provide further personalization of the system.*

Key words: *Computer mouse usage characteristics, mouse dynamics, behavioural patterns, authentication, learning styles prediction.*

INTRODUCTION

The idea of e-learning systems might suffer from dishonest behaviour of students, especially where the outcome of online assessment is certification or degree. One-time authentication using password cannot defend against remote user impersonation [11]. The way of reinforcing password protection of an account could be done using biometrics, specifically behavioural characteristics of users. Standard input devices provide data such as keyboard and computer mouse usage characteristics that show good results in proving identity either when accessing account or continuously after his/her logging in [3].

In this paper we propose a method to check student's identity in sessions such as completing tests based on mouse usage patterns. We provide preliminary results based on our first experiment in a university e-learning system. We analyzed suitability of characteristics (movement velocity, click duration, etc.) for authentication and reliability of the method based on these characteristics. In our subsequent experiment we also examined the possibility of predicting Index of Learning Styles based on mouse usage patterns that could be used with great advantage in personalizing educational systems. We enclose performance description and results of the constructed models.

RELATED WORK

Authentication using behavioural patterns has been studied by number of researchers. The purpose of such methods is to improve security of password protected accounts. In general, scheme of authentication system includes gathering data of an authorizing user and comparing it with the user's template model stored in a database in order to prove or reject his/her identity. Studied behavioural patterns generated by keyboard show decent performance in the terms of security [10, 2, 13]. Web-based applications (and e-learning systems with no exception) are controlled by computer mouse most of the time, so we put emphasis on this area of research.

A basic method proposed in [12] embraced gathering of mouse events and calculating characteristics such as distance, duration and angle for a window of N points. Template of a user is represented by a decision tree which is used to classify new measured data if they belong to the user. In other works mouse events are organized into various high-level actions – *strokes* for bordered movement data [7], four common actions *point & click, drag & drop, movement and silence* [1] or more complex hierarchy of actions [5]. Calculated characteristics for movement actions are based on distance, duration and angle between two consecutive points.

In our previous work [4] we examined suitability of mouse characteristics for identification/authentication in an e-shop system. Data are organized into four types of intended actions by user – clicks, movement strokes, scrolling strokes, silence (no activity). The clicks and silence records are described by duration, scrolling strokes by

velocity and acceleration, movement strokes by six features – velocity, pace, acceleration, direction change curvature and angular velocity.

Performance of biometrics systems for identity verification are compared using error rates FAR (false acceptance rate) and FRR (false reject rate). FAR expresses mistaking biometrics measurements from two different persons to be from the same person while FRR. Both FAR and FRR are functions of threshold *t* and there is a trade-off between the error rates [9]. Usually EER (equal error rate) is estimated, an intersect of FAR and FRR functions. The works [12, 7, 1, 5] stated above mention error rates to be 0.4%/1.8% (FAR/FRR), 6.2% (ERR), 2.5% (ERR) and 7.5% (ERR).

Besides security issues, monitoring user's mouse and computer usage in e-learning environment could be used to detect emotional and affective state of students such as feeling bored, frustrated or excited [8].

PROPOSED CHEATING DETECTION METHOD

Our method is similar to one proposed in our previous work [4]. There are four steps in the process of verification. Firstly, mouse events are collected. Then, high-level mouse actions are formed from the raw data. Thirdly, user model of a current user is constructed. The difference is in the last step, when the test user model from current session is compared to the template model of the same user. If the models match, identity of the user is proven, otherwise the current user is marked as impostor.

In the context of e-learning system, template user model is formed progressively during user's interaction with the system. When a special session such as completing of a test is finished, constructed model based on acquired data is compared with template model in order to label those submitted test which were completed by illegitimate persons.

The user model is represented by vectors holding average, deviation and count for each of 16 features calculated from observed mouse actions: 1 characteristic for action click (duration), 1 for silence (duration), 10 for movement strokes and 4 for scrolling strokes. We can calculate velocity, acceleration, direction change, curvature and angular velocity for every measured point of the stroke, thus the movement stroke is described by average and deviation of five characteristics mentioned above. Analogously, scrolling stroke can be described by average and deviation of velocity and acceleration.

For classification of user's legitimacy (genuine user/impostor) we use *t statistics* of the Welch's test to get the distance of two vectors (test user model and template). Besides average value, also standard deviation and count of collected actions are taken into account. The distance is calculated as:

$$t = \sum_{i \in \mathit{features}} \frac{\mu_{c_i} - \mu_{t_i}}{\sqrt{\frac{\sigma_{c_i}}{N_{c\,i}} + \frac{\sigma_{t_i}}{N_{t\,i}}}} w_i \,,$$

where μ_c, μ_t are vectors of average values of 16 features of test user and his/her corresponding template, σ_c, σ_t are vectors of standard deviations and N_c, N_t are vectors of counts of observed actions. The distance is weighted by value of distinctiveness of the *i*-th characteristic. The distinctiveness values are computed as a ratio of pairs of users differing in the characteristic and all pairs. If the distance is above threshold *t,* session is marked as invalid.

EXPERIMENT ON METHOD PERFORMANCE

We conducted our first offline experiment in web-based educational system ALEF [14] being used at the faculty in few courses. We collected mouse data from 21 users varying in number of performed actions in system from 150 to 5000 with average 1016

(261 movement strokes, 312 clicks, 442 silence records). We omitted scrolling strokes because of small number of observed actions resulting from UI design of the system.

We examined distinctiveness of the characteristics in order to understand its contribution to identity verification (see Figure 1). To study suitability of the characteristics across different domains, we compared distinctiveness obtained in e-learning systems and to those obtained in e-shop in previous work. The similarity observed is that movement speed and acceleration characteristics have values around 0.6 for both average and deviation while angular characteristics have rather good values for deviation only.

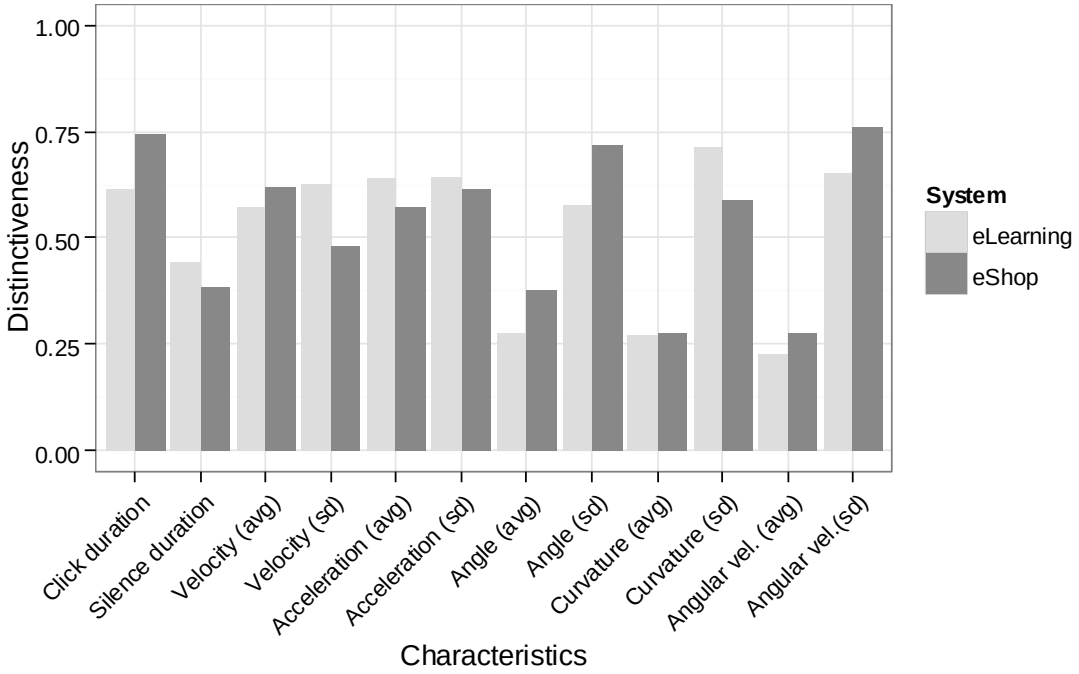

Figure 1. Comparison of distinctiveness values of characteristics obtained from e-shop and e-learning system

To evaluate performance of our method we split data to a bigger training set and a smaller testing set for each user. The size of the testing set is 75 actions (20 movement strokes, 15 clicks, 40 silence records) and is chosen due to the user with minimum amount of actions 150. To estimate FAR using such small dataset we split shuffled data multiple times. The charts in the Figure 2 show error rates FAR and FRR estimated in multiple points of threshold *t*. The first chart shows results when no weights were applied to characteristics and the ERR is estimated to be 27.8%. In the second case, characteristics were weighted by squared value of their distinctiveness. The ERR is 22.8%.

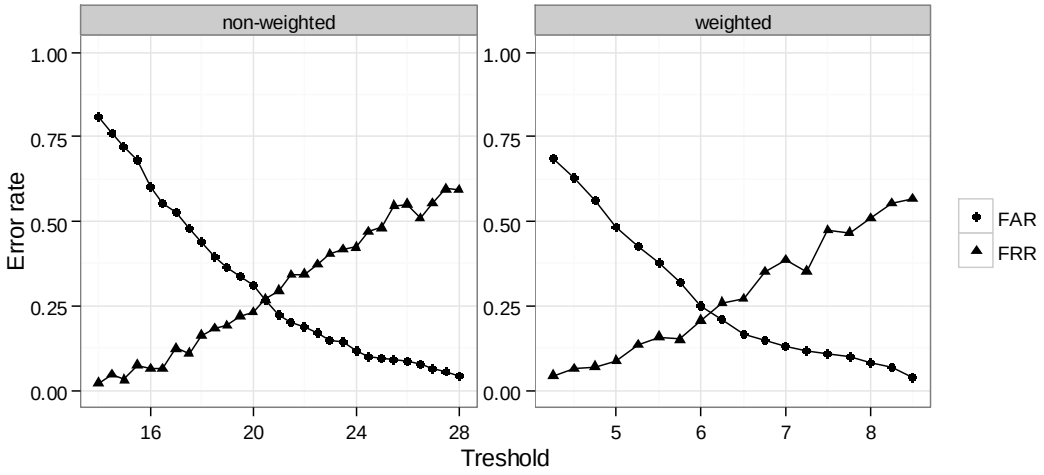

Figure 2. Estimated error rates FAR and FRR in multiple points of threshold t

EXPERIMENT ON LEARNING STYLES PREDICTION

ALEF is a personalized system which adaptation and recommendation is based also on learning style indicators of a student along with other inputs. Our assumption is that learning styles are related to mouse usage characteristics and consequently could be predicted. 14 students filled in ILS (Index of Learning Styles) [6], an questionnaire to access preferences on the four dimensions of the Felder-Silverman learning style model. The four dimensions are following: 1.) *sensing – intuitive*, 2.) *visual – verbal*, 3). *active – reflective*, 4.) *sequential – global*. Our representation of learning styles is simplified to 3 values for each axis. Preference on the one or another learning style within a dimension is marked with -1 or 1, no preference is marked as 0.

We constructed and evaluated models for predicting learning styles of a user. Four multilayered perceptron models were trained each classifying preference on one of the dimensions. We reduced set of input attributes (mouse usage characteristics) using greedy stepwise method in order to avoid overfitting of the models. As we possessed just limited set of data we evaluated models using threefold cross-validation. The attributes used for classification and precision of the models are summarized in Table 1. The best prediction was achieved in dimension *visual – verbal* with precision 92.86%.

Table 1. Selected characteristics and precision of classification of learning styles preferences using multilayered perceptron

Dimension	Input characteristics	Precision
sensing – intuitive	Silence duration	85.7%
visual – verbal	Velocity (std), Click duration	92.9%
active – reflective	Acceleration (avg), Velocity (avg)	71.4%
sequential – global	Curvature (avg), Click duration	64.3%

CONCLUSIONS AND FUTURE WORK

In our work, we described our method for detection of sessions when person interacting with the system is not legitimate. The method is based solely on his/her mouse usage during the interaction. We evaluated our method using data collected in e-learning system in order to develop a module for cheating detection. The error rate of the identity verification was estimated to be 22.8% FAR and FRR in our first experiment on 21 students. The result might be affected by rather small dataset acquired at the end of the academic term. In our future work we plan to collect data long-term and enhance our method using advanced techniques of machine learning.

In this paper we show that the computer mouse characteristics are not only distinguishing one person from another, but also can be used to determine group the person belongs to. We experimented with predicting learning styles resulting in 92.9% precision of determining one out of four dimensions (visual–verbal). It is challenging task for us to develop a method that builds such a user model in implicit way in future.

REFERENCES

[1] Ahmed, A.A.E., Traore, I.: A New Biometric Technology Based on Mouse Dynamics. In: IEEE Transactions on Dependable and Secure Computing, (2007), vol. 4, no. 3, pp. 165–179.

[2] Bergadano, F., Gunetti, D., Picardi, C.: User authentication through keystroke dynamics. In: ACM Transactions on Information and System Security, (2002), vol. 5, no. 4, pp. 367–397

[3] Chudá, D., Ďurfina, M.: Multifactor authentication based on keystroke dynamics. In: Proceedings of the International Conference on Computer Systems and Technologies and Workshop for PhD Students in Computing, (2009), pp. 1–6.

[4] Chudá, D., Krátky, P.: Usage of computer mouse characteristics for identification in web browsing. In: CompSysTech '14 Proceedings of the 15th International Conference on Computer Systems and Technologies, (In print).

[5] Feher, C. et al.: User identity verification via mouse dynamics. In: Information Sciences, vol. 201, (2012), pp. 19 – 36.

[6] Felder, R., Spurlin, J.: Applications, reliability and validity of the index of learning styles. In: International journal of engineering education, vol. 21, no. 1, (2005), pp. 103-112.

[7] Gamboa, H., Fred, A.: A behavioral biometric system based on human-computer interaction. In: Proceedings of SPIE, (2004).

[8] Lee P., Tsui W., Hsiao T.: A low-cost scalable solution for monitoring affective state of students in e-learning environment using mouse and keystroke data. In: Proceedings of the 11th international conference on Intelligent Tutoring Systems ITS'12, (2012), pp. 679-680.

[9] Jain, K., Ross, A., Prabhakar, S.: An Introduction to Biometric Recognition. In: IEEE Transactions on Circuits and Systems for Video Technology, (2004), vol. 14, no. 1, pp. 4–20.

[10] Joyce, R., Gupta, G.: Identity authentication based on keystroke latencies. In: Communications of the ACM, (1990), vol. 33, no. 2, pp. 168–176.

[11] Moini, A., Madni, A.: Leveraging Biometrics for User Authentication in Online Learning: A Systems Perspective. In: Systems Journal, IEEE, vol. 3, no. 4, (2009), pp. 469-476.

[12] Pusara, M., Brodley, C.E.: User re-authentication via mouse movements. In: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security - VizSEC/DMSEC '04, (2004), pp. 1–8.

[13] Shanmugapriya, V., Padmavathi, G.: Keystroke Dynamics Authentication Using Neural Network Approaches. In: Information and Communication Technologies, Communications in Computer and Information Science, vol. 101, (2010), pp. 686 – 690.

[14] Šimko, M., Barla, M., Bieliková, M.: ALEF: A framework for adaptive web-based learning 2.0. In: Key Competencies in the Knowledge Society, IFIP Advances in Information and Communication Technology, vol. 324, (2010), pp. 367-378.

ACKNOWLEDGEMENT

This work was partially supported by the Scientific Grant Agency of the Slovak Republic, grant No. VG1/0971/11 and is the partial result of the Research & Development Operational Prog. for the project ITMS 26240220039, co-funded by the ERDF.

ABOUT THE AUTHOR

Ing. Peter Krátky, Institute of Informatics and Software Engineering, Faculty of Informatics and Information Technology, Slovak University of Technology in Bratislava, Slovak Republic, Phone: +421 902 680 177, E-mail: kratky@fiit.stuba.sk.

The paper has been reviewed.