A Proposal for Continuous and Silent User Authentication Through Mouse Dynamics and Explainable Deep Learning

Giovanni Ciaramella*
IIT-CNR
Pisa, Italy

Giacomo Iadarola†
IIT-CNR
Pisa, Italy

Fabio Martinelli‡
IIT-CNR
Pisa, Italy

Francesco Mercaldo§
University of Molise & IIT-CNR
Campobasso, Italy

Antonella Santone¶
University of Molise
Campobasso, Italy

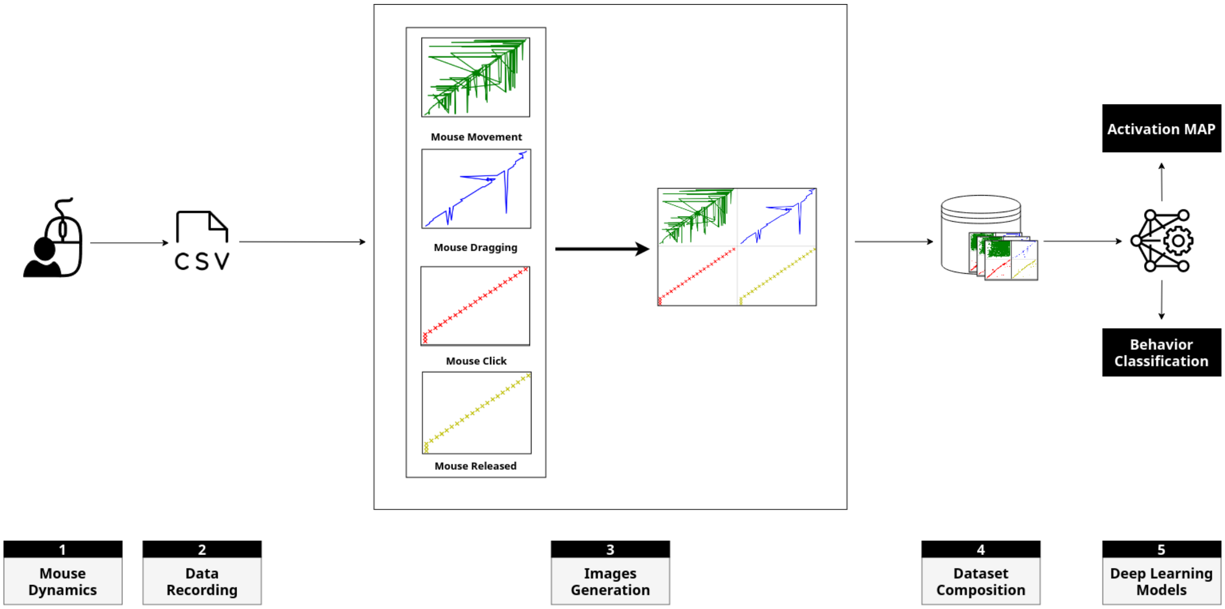

Figure 1: The proposed method for continuous and silent user authentication.

Abstract

Over the years, the number of compromised accounts dramatically increased. Many types of authentication methods have been introduced to avoid this type of attack. In particular, recently taken hold biometric-based such as physical-biometric and behavior-biometric. The idea at the bottom of the last technique is that each person has a unique behavior. Starting from the touch dynamics, and keyboard dynamics nowadays, one of the most promising investigation areas is currently represented by mouse dynamics. Opposite to the other techniques, mouse dynamics require simpler hardware to capture the biometric data without using sensitive data from the users. In this paper, we propose an approach for continuous and silent user authentication based on mouse dynamics and explainable deep learning. We generate a set of images starting from mouse dynamics, and we input a deep learning model to discriminate between legitimate and malicious users. We also propose to adopt the Gradient-weighted Class Activation Mapping, to allow highlighting the areas of the images which are responsible for a specific legitimate/attack prediction, thus providing explainability behind the model classification. The preliminary experimental analysis based on ten different users shows that the proposed method can be promising in silent and continuous user authentication.

Index Terms: Computer security—Intrusion detections—Privacy; Image Classification—Deep Learning

1 Introduction and Related Work

The number of attacks on personal accounts has grown over time. Numerous user authentication techniques have been created throughout the years to avoid it. Among these, there is biometric-based authentication. This type of technique exploits physical-biometric or behavior-biometric for user recognition. While physical biometrics rely on the uniqueness of specific physical attributes among individuals, such as the face, ear, iris, and fingerprints, the second authentication technique is predicated on the notion that each human exhibits a distinct behavior. For instance, touch dynamics, keyboard dynamics, and mouse dynamics belong to this second category. In particular, in this paper we focus on mouse dynamics, consisting of the iteration of the user with a specific system using a mouse. Compared to the other techniques, the latter does not require any special hardware to capture the biometric data [3], and it does not need sensitive data from the users. This last happens because using keystroke dynamics, for example, provides that the users type their password or other information which may contain sensitive data [1].

*e-mail: g.ciaramella1@studenti.unimol.it
†e-mail: giacomo.iadarola@iit.cnr.it
‡e-mail: fabio.martinelli@iit.cnr.it
§e-mail: francesco.mercaldo@unimol.it, francesco.mercaldo@iit.cnr.it
¶e-mail: antonella.santone@unimol.it

record timestamp	client timestamp	button	state	x	y
0.0,0.0		NoButton	Move	613	140
0.232000112534	0.234000000171	NoButton	Move	262	2
0.335999965668	0.342999999877	NoButton	Move	361	97
0.624000072479	0.436999999918	NoButton	Move	451	140

Figure 2: A piece of CSV file used as an example.

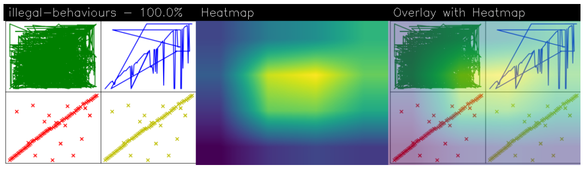

Figure 3: The image belongs to the class *illegal behaviors* and was obtained after applying Grad-CAM on 7ca81640383dbfa489220029f41d6ac5.png.

For these reasons, in this paper, we propose a method for continuous and silent user authentication based on mouse dynamics and deep learning. In a nutshell, starting from a dataset composed of *legal behaviors* and *illegal behaviors* (explained in Section 2), we generate four single images to represent the behaviors of the users, by exploiting a Python script developed by the authors. Four images are proposed for user authentication, obtained from mouse dynamics: in the first one, we draw green lines to show mouse movement, and in the second one the blue lines represent mouse dragging. In the last two images, the red cross represented user clicks, while the yellow cross represented mouse release. At the end of the generation of the four single images (symbolizing a user session), we combined all four images into one. In Figure 1 in point 3 (i.e., Image Generation) an example of the steps explained before is shown. Furthermore, we used the Gradient-weighted Class Activation Mapping (Grad-CAM) approach to emphasize the area of the images under study that is responsible for a certain model prediction.

2 The Proposal

To perform the first step reported in Figure 1, we have chosen a dataset built in 2016, provided by Fülöp et al. that outlined some tasks, and the users logged to a remote server where they executed them, to collect the mouse interactions between users and the system [2]. Following data capture, the data were saved in CSV files with the following structure: record timestamp in second, client timestamp in second, the current condition of the mouse buttons, additional information about the current state of the mouse, and x-y coordinate of the cursor on the screen. This process has been applied for every ten users, and at the end, each CSV file created was labeled as *legal behaviors* and *illegal behaviors*. In Figure 2 we report a small piece of a CSV file obtained after the challenges proposed by the authors as an example.

2.1 Dataset Composition

We have used a dataset named “Balabit Mouse Dynamics Challenge Data Set” [1] which was composed of CSV files obtained from ten different users. From that, we have generated the images. For image generation, we developed a script that goes to insert the x and y coordinates for each file into each specific list, which takes the name of the action done by the user. The coordinates represent the most significant data in a row. After graph creation for each list, they are joined into a single image with a PNG extension. After that, we divided them into two classes, such as *legal behaviors* and *illegal behaviors* (i.e., the classes to discriminate). The latter was possible, using a file named *public_labels.csv* also contained in the GitHub repository. We obtained, i.e. 405 for *illegal behaviors*, and 1271 for *legal behaviors*: in this preliminary experimental evaluation we randomly gathered a subset of the session from the exploited dataset. Because of this, we consider the data augmentation technique. Thanks to this approach, we increased the number of components in our dataset. In particular, we developed a Python script able to obtain new images by performing the zoom, rotation, flip, height shift, and brightness modification for each image stored in the dataset. In this case, we came up with 8000 elements for each class. This allows for obtaining a balance of the dataset. After this phase, we submitted our dataset to a deep learning model for a preliminary evaluation, as shown in Figure 1 where the proposed method is shown.

3 Preliminary Evaluation

In this section, we conduct a preliminary evaluation using the VGG16 model. In particular, we considered 150×3 as Image Size, Batch Size equal to 64, 20 epochs, and a learning rate value set at 0.0001 for training a model aimed to discriminate between *legal behaviors* and *illegal behaviors*. Using them, we achieved a precision, accuracy, and F-Measure value equal to 0.902. At the same time, the loss value is 0.428, and the AUC (Area Under the Curve) we reached is 0.953. We conclude that this model has achieved good performances per class. The class labeled *illegal behaviors* found 2179 true positives, 2151 true negatives, 249 false positives, and 221 false negatives. In particular, for this class, the accuracy, recall, f-measure, and AUC values equal 0.902, while the value referred to the precision was 0.897. About the second class, named *legal behaviors* the model retrieved 2151 true positives, 2179 true negatives, 221 false positives, and 249 false negatives. Specifically relating to this class we reached an accuracy, precision, f-measure, and AUC equal to 0.902, while the recall value was 0.896. After the VGG16 model execution, we proceeded to use the Grad-CAM to understand the reliability of classification and which areas of the image are useful for the prediction. In Figure 3 we respectively show the PNG image, the activation map, and the image generated by overlaying the initial PNG image with its activation map. The heat map takes into account three distinct shadows: yellow, green, and blue. The model is uninterested in the blue color, even though it is used to draw attention to a certain area of the image. The model is most interested in the portions of the image that are yellow, but in the end, the green color is chosen to denote the areas in the middle.

4 Conclusion and Future Work

In this paper, we proposed a methodology for continuous and silent user authentication based on mouse dynamics and deep learning. In the preliminary evaluation, we resort to the VGG16 model, achieving good accuracy and precision values. We also provided the Grad-CAM to interpret the obtained outputs. In future studies, we would consider different models to improve the performances. Furthermore, we would consider more data for model training and evaluation.

Acknowledgments

This work has been partially supported by MIUR SecureOpenNets, EU SPARTA, CyberSANE, and E-CORRIDOR projects.

References

[1] M. Antal and E. Egyed-Zsigmond. Intrusion detection using mouse dynamics. *IET Biometrics*, 8(5):285–294, 2019.

[2] Á. Fülöp, L. Kovács, T. Kurics, and E. Windhager-Pokol. Balabit mouse dynamics challenge data set 2016. `https://github.com/balabit/Mouse-Dynamics-Challenge`. Accessed: 2022-06-30.

[3] S. Mondal and P. Bours. Continuous authentication using mouse dynamics. In *2013 International Conference of the BIOSIG Special Interest Group (BIOSIG)*, pp. 1–12. IEEE, 2013.

[1] https://github.com/balabit/Mouse-Dynamics-Challenge