proceedings

Proceedings

A First Approach to Authentication Based on Artificial Intelligence for Touch-Screen Devices [†]

Arturo Silvelo *, Daniel Garabato, Raúl Santoveña and Carlos Dafonte

CITIC, Department of Computer Science and Information Technologies, University of A Coruña, Campus de Elviña S/N, 15071 A Coruña, Spain; daniel.garabato@udc.es (D.G.); raul.santovena@udc.es (R.S.); dafonte@udc.es (C.D.)

* Correspondence: arturo.silvelo@udc.es

† Presented at the 3rd XoveTIC Conference, A Coruña, Spain, 8–9 October 2020.

Published: 18 August 2020

Abstract: Most authentication schemes follow a classical approach, where the users are authenticated only once at the beginning of their sessions. Therefore, it is not possible to verify the legitimate use of such a session or to detect any usurpation. In order to address this issue, we propose a second-phase authentication scheme that provides not only continuous user authentication during their sessions, but also in a transparent manner, since no additional or intrusive hardware is required. To this purpose, a novel approach was applied to create specific user profiles by means of different Artificial Intelligence techniques. In this work, we aim to study the feasibility of such an authentication scheme, so that it could be applied to a real time environment in order to verify the identity of the actual user against the legitimate user profile.

Keywords: authentication; artificial intelligence; cybersecurity

1. Introduction

Since the beginning of Information Technologies, authentication models have been an essential component for information security [1] and they have been adapted to the new devices and technologies that have appeared over the years, such as mobile phones, which are nowadays an indispensable tool to perform any daily operation. However, the authentication mechanisms commonly used present certain issues that can lead to security incidents related to weak or lost passwords. For these reasons, new and more secure authentication systems [2,3], such as the biometric ones, have been implemented, making use of unique human traits as passwords. Even so, these authentication systems continue to present a common problem, since they only verify the legitimacy of the user at the beginning of the session and not during it.

In this work, we propose a continuous authentication model which is based on the monitorization of the users' behavior [4] during the usage of a mobile device. Such a model is presented as a second authentication factor, which verifies the legitimacy of the user in a transparent manner, being able to detect if the user who is making use of the session is the one that was originally authenticated. For this purpose, it was necessary to create a multiplatform application that gathers data from the available motion sensors (mainly, accelerometer and gyroscope) and the touch-screen to generate a specific profile for each user by means of Artificial Intelligence (AI) techniques.

2. Methods

In order to conduct this experiment, we developed an application that collects information from the events associated with the use of the device. Those events related to motion sensors were grouped in time windows, whereas the touch-screen ones were grouped into gestures (swipe, rotate, tap, press, pinch, and pan) in order to seek for patterns to authenticate users. The data collected over three months were processed to extract a set of features, but first we needed to carefully analyze and treat such data in order to fit them to the classification techniques that were used. Some processes performed were the treatment of null and empty values, data standardization, definition of numerical/categorical variables, as well as feature extraction and selection.

Following this procedure, we obtained around 50 genuine features and many polynomial derived ones. Hence, feature selection was a key task in this phase and different techniques, such Random Forest or Recursive Feature Elimination processes, were used to assign different weights to the features, so that the most relevant ones could be identified in order to build the models.

Then we can feed some different well-known classification techniques (such as Random Forest [5], Support Vector Machines [6] and Multi-layer Perceptrons [7]) with the selected features in order to create a profile for each legitimate user in the system. These techniques require a training process so that they can appropriately fit the data, and the best configuration for each one was determined via hyper-parameterization and cross-validation procedures.

3. Results

Table 1 shows different common metrics used for classification tasks (accuracy, precision, recall and F1 Score). Among those metrics, we considered the precision as the most relevant one for our task, since it measures the number of intrusions into the system. These results show that the average response for our system is over 80% in terms of precision, and the F1 score is near 75%. The lowest score is obtained for the recall metric, which measures the identification of legitimate users as impostors.

Table 1. Results for each grouped by selected algorithms and events.

Users	Accuracy	Precision	Recall	F1 Score
01	80.29%	81.18%	78.85%	80.00%
02	78.11%	85.57%	68.78%	76.26%
03	80.17%	90.91%	69.67%	78.89%
04	81.82%	92.28%	70.92%	80.20%
05	79.62%	81.09%	76.90%	78.94%
06	72.97%	80.65%	64.10%	71.43%
07	52.50%	62.50%	43.48%	51.28%
08	63.12%	69.35%	51.81%	59.31%
09	68.94%	80.00%	59.46%	68.22%
10	84.07%	89.73%	78.30%	83.63%
11	83.75%	89.86%	76.54%	82.67%
12	71.92%	82.00%	56.16%	66.67%
13	76.19%	80.99%	68.45%	74.19%
14	82.85%	90.38%	75.20%	82.10%
15	81.43%	86.16%	76.11%	80.83%
16	76.07%	80.90%	69.76%	74.92%
17	77.84%	84.83%	68.72%	75.93%
18	76.85%	80.29%	69.62%	74.58%
Total	**76.03%**	**82.70%**	**67.94%**	**74.45%**

4. Conclusions and Future Work

As can be observed in Table 1, it has been demonstrated that a user's behavior can be used for authentication purposes. Although the recall metric shows that there is a considerable ratio of legitimate user misidentification, which may prevent this method as a primary authentication scheme, the obtained precision score encourages us as to its usage as a second authentication scheme that monitors user activity in a continuous and transparent manner over the entire session, since true impostors are usually detected. Such a system may have conservative behavior, and sometimes an alert would be raised for a legitimate user, but it only aims at detecting intrusions into the system once the user is already authenticated by a primary authentication scheme, such as a user/password one. Then, in case any usurpation is detected, the system could require the user to re-authenticate using the primary scheme, or even raise some notifications to the system administrators so that they can take further action.

In order to implement such an authentication scheme, we plan to use a streaming platform capable of handling events in near real time (sending, processing and storing the events for retraining against AI models (Figure 1)), so that the identity of the actual user can be verified in a short-time period.

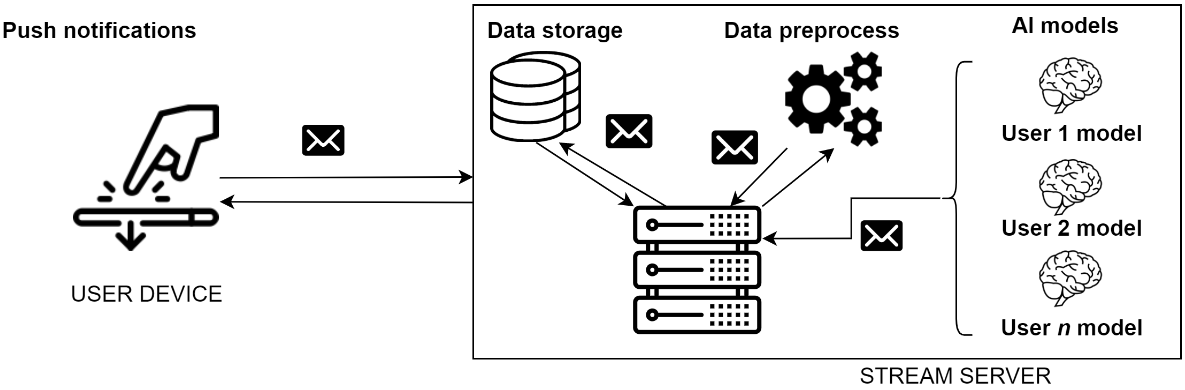

Figure 1. Authentication scheme for streaming platform.

Funding: This work has been mainly funded by the contracts CITIC-ACATIA, and CITIC-ACATIA2 established with the private entity ODEENE Ingeniería.

Acknowledgments: We also wish to acknowledge the support received from the CITIC as a Research Centre of the Galician University System is financed by the Conselleria de Education, Universidades e Formacin Profesinal (Xunta de Galicia) through the ERDF (80%), Operational Programme ERDF Galicia 2014–2020 and the remaining 20% by the Secretaria Xeral de Universidades (Ref. ED431G 2019/01), the research group fund ED431B 2018/42, and the Ministerio de Educación Cultura FPU16/03827 grant.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Stallings, W.; Brown, L. *Computer Security: Principles and Practice*, 1st ed.; Prentice Hall Press: Upper Saddle River, NJ, USA, 2007.
2. Barkadehi, M.H.; Nilashi, M.; Ibrahim, O.; Zakeri Fardi, A.; Samad, S. Authentication systems: A literature review and classification. *Telemat. Informatics* **2018**, *35*, 1491–1511, doi:10.1016/j.tele.2018.03.018.
3. Garabato, D.; García, J.; Nóvoa, F.; Dafonte, C. Mouse Behavior Analysis Based on Artificial Intelligence as a Second-Phase Authentication System. *Proceedings* **2019**, *21*, 29, doi:10.3390/proceedings2019021029.
4. ul Haq, M.E.; Awais Azam, M.; Naeem, U.; Amin, Y.; Loo, J. Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing. *J. Netw. Comput. Appl.* **2018**, *109*, 24–35, doi:10.1016/j.jnca.2018.02.020.
5. Breiman, L. Random forests. *Mach. Learn.* **2001**, *45*, 5–32.
6. Cortes, C.; Vapnik, V. Support-vector networks. *Mach. Learn.* **1995**, *20*, 273–297.
7. Rumelhart; David, E.; James, M.; James, L. *Parallel Distributed Processing: Explorations in The Microstructure of Cognition. Volume 1. Foundations*; MIT Press: Cambridge, MA, USA, 1986.