Method of user identification based on dynamic characteristics of mobile device hardware

A A. Salomatin*

V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Profsoyuznaya street, 65, 117997, Moscow, Russia

Abstract. The paper considers a method of user identification based on dynamic characteristics of mobile device hardware. The characteristics include battery state, battery charge level, battery charging status, memory utilization and device orientation. All indicators can change their values over time and allow to form data sets from them for processing and analyzing in the task of user identification. The correctness of identification is determined by testing statistical hypotheses based on three criteria: one-sample Student's t-criterion, one-sample criterion for testing the hypothesis about the numerical value of variance, Kolmogorov-Smirnov criterion, as well as calculating the resulting probability, which depends on the probabilities of correct identification for each of the criteria and selected significance levels. The application of the method can improve the efficiency of user identification, which is confirmed in the experiment. For generated 100 samples of 3600 values for each investigated dynamic indicator and one data set, user identification with high value of the resulting probability was successfully performed. The results of the work are useful for their analysis and practical application, as well as the development of new methods of identification and authentication.

1 Introduction

Information security of mobile device infrastructure is currently attracting more and more attention from researchers. The number of people using mobile devices on a daily basis is huge. Mobile devices are popular all over the world and are used almost everywhere. Therefore, it is an important issue to provide a high level of security for users, where they do not have to worry about their data falling into the hands of cybercriminals.

To address the issue, new methods are being developed to detect and recognize threats related to authentication and identification of mobile device users [1-7]. Effective authentication and identification of users today is relevant because it reduces the risks of threats associated with loss and theft of information in many spheres of human activity.

There are many different authentication methods. The effectiveness of long-established password-type methods decreases over time due to emerging new attack methods, so they are supplemented and/or replaced by new methods.

* Corresponding author: aleksandr.salomatin@phystech.edu

One of the promising approaches to user identification and authentication is becoming the use of digital footprinting, which can include various static and dynamic characteristics of user devices [8-16]. Characteristics considered may include browser attributes, activity logs, keyboard and computer mouse handwriting, and others.

Despite the variety of methods of user identification based on digital footprints, the effectiveness of authentication can still be improved by increasing the accuracy of identification. It is possible to develop a new method of user identification based on their digital footprint, which will include new characteristics not previously used for this purpose.

In the current work it is proposed to use dynamic characteristics of the hardware of mobile devices of users, which, although they require a lengthy collection of primary data, but have a stricter link to users compared to other parameters, thereby providing reliable identification.

The purpose of the work is to improve the efficiency of identification of mobile device users by developing a method of user identification based on the dynamic characteristics of mobile device hardware.

2 Identification based on the dynamic characteristics of mobile device hardware

Suppose that for one user of a mobile device, its dynamic characteristics are defined at time instants $t_k = \{t_{1k}, t_{2k}, t_{3k}\}$ with hours, minutes and seconds respectively $\{x_1(t_k), x_2(t_k), \ldots, x_N(t_k)\}$. At time points $T_k = \{T_{1k}, T_{2k}, T_{3k}\}$ new features $\{r_1(t_k), r_2(t_k), \ldots, r_N(t_k)\}$ were received. We need to find. $y(j)$, where $y(J(t_i))$ is a binary function from the set of features J collected at time points ti that determines the correct identification of the user. When $y(j) = 1$, the user is correctly identified, and when $y(j) = 0$, the user cannot be correctly identified, i.e., either additional verification is needed or the user may be a malicious stranger.

First of all, let us determine what dynamic characteristics of the hardware will be investigated. It is proposed to investigate the following time-varying indicators:

1. Battery state. It defines the state of the battery at the current moment of time and can take one of 6 values: Good, Overheat, Dead, Over Voltage, Unspecified Failure, Unknown. The most common value is Good, which means that the battery is in good condition and is not subject to faults or malfunctions. Overheat means that the battery has overheated, which is bad. Dead means that the battery is broken. Over Voltage implies that the battery is in over voltage mode. Faults other than those noted may be identified, then the indicator value is Unspecified Failure. If Unknown is received, no battery condition data has been collected and the condition of the battery cannot be determined definitively.
2. Battery Level. Determines the percentage of battery charge. The value varies from 0 to 100. The maximum battery charge corresponds to - 100 and the minimum battery charge corresponds to 0. The battery charge level can change in two directions. In case the battery is charging - the battery charge level increases, in other cases, if the mobile device is not turned off, the battery charge level decreases.
3. Battery charging status. Can be set to true or false depending on whether the mobile device is currently charging or not.
4. Used memory size. Determines how much memory the mobile device is currently using. The more applications are used and the more processes are running on the device, the higher the value.
5. Device orientation. Determines the orientation of the device at the current moment. There are 4 possible values: Portrait, Landscape, Square, Undefined. Horizontal orientation corresponds to the Portrait value. Vertical orientation corresponds to Landscape. In case the device has the same width and length, the orientation will be

the only one and the value will be Square. There is also a value Undefined, in which the orientation could not be determined.

To determine the correctness of identification for samples of the marked dynamic indicators, statistical hypothesis tests are performed using the following criteria: one-sample Student's t-criterion, one-sample criterion for testing the hypothesis about the numerical value of dispersion, Kolmogorov-Smirnov criterion. In this case, the time periods for the samples should coincide, and there should be data on the reference mathematical expectations and dispersions. As a result of the hypothesis tests, it will be possible to determine five probabilities that determine the correct identification of the user.

Next, by determining the weights for the selected dynamic features that determine their contribution to identification, the final probability of correct identification can be inferred. In case the final probability exceeds the minimum acceptable value, then $y(j) = 1$, otherwise $y(j) = 0$. The boundary value itself should be high, since the method is assumed to provide high identification accuracy.

3 Application of the developed identification method in the experiment

Let's collect 100 sets of dynamic indicators for the experiment for an hour of time each, and then, check the performance of the method on one of the sets, solving the problem of identification. To conduct the experiment, we wrote a program in Android Studio, which reads the user data and writes it to separate files containing dynamic indicators corresponding to the file names. It also produced a display of the corresponding metrics on the device screen, which was updated every second. An example is shown in Fig. 1.

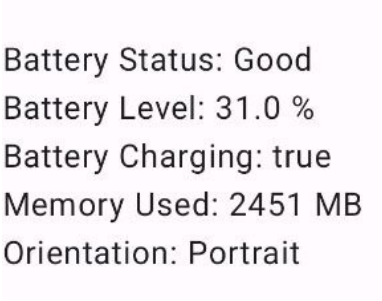

Fig. 1. Output of dynamic indicators of the user's hardware at a specific point in time.

A separate program in Python was written to process and analyze the data.

Let's consider the data of one of the sets. Since the battery state, battery charging status and device orientation did not change during the time interval under consideration, their graphical representation will not be indicative. In turn, the battery level and the amount of memory used changed their values over time and formed characteristic trends, which are represented by the red lines in Fig. 2, 3.

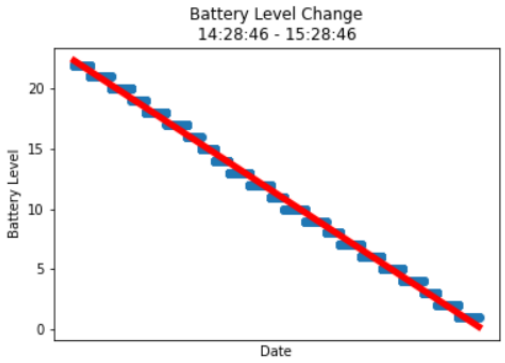

Fig. 2. Changing the battery level.

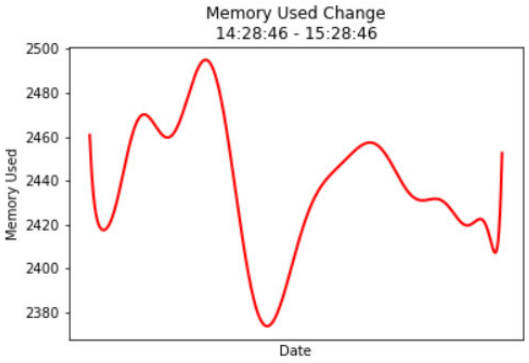

Fig. 3. Changing the amount of memory used for the user data set.

From the graphs can be concluded that in an hour the user actively used the device, which is expressed in the rapid discharge of the battery and changes in the amount of memory used.

To determine the correctness of identification for samples of the noted dynamic indicators, we perform statistical hypothesis tests by criteria at significance levels of 0.01. The results of the calculations are presented in Table 1.

Table 1. Statistical measures of dynamic performance.

Indicator	**Sample average**	**Sample variance**	**Mat. expectation**	**Dispersion**	**Probability of correct identification**
Battery status	1	0	1	0	1
Battery level	11.270	41.059	12.110	44.860	0.970
Battery charging status	0	0	0.100	0.050	0.970
Memory used	2437.746	1628.015	2445.458	1713.432	0.970
Orientation	1	0	1	0	1

Thus, the resulting probability of correct identification is 0.913, which means $y(j) = 1$ and the user can be identified.

4 Conclusion

A method for user identification based on dynamic characteristics of mobile device hardware has been developed and shown to work well in an experiment. User identification based on dynamic characteristics such as battery status, battery charge level, battery charging status, memory utilization and orientation was successfully performed.

This research was funded by Russian Science Foundation, project No 22-21-00846.

References

1. G.V. Kumar, K. Prasanth, S.G. Raj, S. Sarathi, *Fingerprint based authentication system with keystroke dynamics for realistic user*, Sec. Int. Conf. on Current Trends In Engineering and Technology - ICCTET 2014 (Coimbatore, 2014), 206-209
2. N.I. Daud, G.R. Haron, S.S. Othman, *Adaptive authentication: Implementing random canvas fingerprinting as user attributes factor*, 2017 IEEE Symp. on Computer Applications & Industrial Electronics (ISCAIE), (Langkawi, 2017), 152-156
3. A.O. Iskhakova, A.Y. Iskhakov, R.V. Meshcheryakov, R. Bendrau, O. Melekova, *Using a heatmap of user behavior in the problem of identifying the subject of an information security incident*, Proc. of the SPIIRAS (Moscow, 2018), 147-171
4. F. Wang, Y. Zhang, *Study and Design of Intelligent Authentication System Based on Fingerprint Identification*, 2009 Sec. Int. Symp. on Knowledge Acquisition and Modeling, (Wuhan, 2009), 170-173
5. D. Hwang, H. Lee, G. Bae, S. Son, J. Kim, *Fingerprint template management for higher accuracy in user authentication*, 2018 Int. Conf. on Electronics, Information, and Communication (ICEIC) (Honolulu, 2018), 1-4
6. K.A. Abu Bakar, G.R. Haron, *Adaptive authentication based on analysis of user behavior*, 2014 Science and Information Conf. (London, 2014), 601-606
7. T. Keatsamarn, C. Pintavirooj, *Footprint Identification using Deep Learning*, 2018 11th Biomedical Engineering Int. Conf. (BMEiCON) (Chiang Mai, 2018), 1-4
8. A.A. Salomatin, A. Iskhakov, R. Meshcheryakov, *Application of the User's Digital Footprint in the Adaptive Authentication Problem*, 2021 Int. Siberian Conf. on Control and Communications (SIBCON) (Kazan, 2021), 1-5
9. S.V. Akram, S.K. Joshi, R. Deorari, *Web Application Based Authentication System*, 2022 Int. Interdisciplinary Humanitarian Conf. for Sustainability (IIHC) (Bengaluru, 2022), 1439-1443
10. L. Bu, H. Cheng, M.A. Kinsy, *Adaptive and Dynamic Device Authentication Using Lorenz Chaotic Systems*, 2018 IEEE 61st Int. Midwest Symp. on Circuits and Systems (MWSCAS) (Windsor, 2018), 976-979
11. E. Davarci, E. Anarim, *User Identification on Smartphones with Motion Sensors and Touching Behaviors*, 2022 30th Signal Processing and Communications Applications Conf. (SIU) (Safranbolu, 2022), 1-4
12. T. Gan, F. Lin, C. Chen, Y. Guo, Y. Zheng, China Communications **10(3)**, 76-81 (2013)
13. A. Salomatin, A. Iskhakov, R. Meshcheryakov, *Formation of a digital footprint based on the characteristics of computer hardware to identity APCS*, Users Proc. of the 2021 Int. Russian Automation Conf. (RusAutoCon) (Sochi, 2021), 314-320

14. K. Takasu, T. Saito, T. Yamada, T. Ishikawa, *A survey of hardware features in modern browsers: 2015 Edition*, Proc. of the 2015 9th Int. Conf. on Innovative Mobile and Internet Services in Ubiquitous Computing (Santa Catarina, 2015), 520-524
15. A. ElBanna, N. Abdelbaki, *Browsers fingerprinting motives, methods, and countermeasures*, Proc. of the 2018 Int. Conf. on Computer, Information and Telecommunication Systems (CITS) (Alsace, 2018), 978-982
16. S. Dong, F. Farha, S. Cui, H. Ning, J. Ma, *CPG-FS: A CPU perfomance graph based device fingerprint scheme for devices identification and authentication,* Proc. of the 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing (Fukuoka, 2019), 266-270