Authenticating Users Based on How They Pick up Smartphones

Kamil BURDA*

Slovak University of Technology in Bratislava
Faculty of Informatics and Information Technologies
Ilkovičova 2, 842 16 Bratislava, Slovakia
kamil.burda@stuba.sk

Abstract. User identification and authentication methods become increasingly reliant on the use of biometrics – observing the user's physiological or behavioral characteristics – to reduce user inconvenience and increase security. On smartphones, one may leverage the potential of touch screen and motion sensors (accelerometer and gyroscope) to extract useful behavioral biometrics. This paper presents a novel approach to authenticate users based on the way users pick up a smartphone on a table or in their front pockets, an activity performed frequently every day, using the smartphone's accelerometer sensor.

1 Introduction

Mobile devices, especially smartphones, have become nearly ubiquitous, with people using them every day for numerous applications, such as messaging or social media. It is easier more than ever to compromise the security of smartphones and users' personal data therein given that users deliberately choose weaker authentication mechanisms for convenience. This is understandable, as traditional mechanisms, such as text-based passwords, are difficult and error-prone to type on small touch screens. Lock patterns, a popular choice for a phone unlock mechanism due to the simplicity of drawing patterns, can be deduced by tracking the corresponding smudges on the touch screen.

One way to enhance the security of devices without disrupting the user experience is to track user's biometric characteristics. Physiological biometrics determine who the user is, such as user's fingerprints, irises or face. Behavioral biometrics observe the user's behavior, such as typing behavior (also called keystroke dynamics) or movements (hand gestures, walking). While behavioral biometrics are considerably less accurate compared to physiological, they do not require any additional hardware, are more difficult to replicate than physiological biometrics and are more resistant against differences in the environment (such as the amount of light in the surroundings or background noise) [14]. Behavioral biometrics are therefore generally recommended to be used as an additional security mechanism or a part of a multi-modal biometric system. Another use of biometrics is to adapt content and user interface of applications for each user individually.

---

* Doctoral study programme in field: Software Engineering
Supervisor: Assoc. Professor Daniela Chudá, Institute of Informatics and Software Engineering, Faculty of Informatics and Information Technologies STU in Bratislava

In order for a system (an application on a device) to identify or authenticate users based on biometrics, the system needs to observe the user and create a user model. The system first requires the user to perform activities sufficiently long enough so that the system is then able to train itself to recognize the user. The trained data is called a user template. Once trained, the system then logs user's activities from chosen devices or sensors (such as accelerometer for movement-based biometrics). The logged data are processed to output useful features (such as mean acceleration or velocity for movements). The values of extracted features are then matched against the user template (using statistical methods or classifiers). Successfully matching (classifying) the user may result in successful user identification or authentication, depending on the goal of the system. For user authentication, the system determines whether the extracted features match the user's template. User identification is a more difficult task, as the system must distinguish each stored template in the system to match the extracted features.

The accuracy of a biometric system is usually evaluated by the False Acceptance Rate (FAR) and False Rejection Rate (FRR). FRR is the probability that the system fails to recognize the authorized user. FAR is the probability that the system incorrectly recognizes an unauthorized user as an authorized user. FAR and FRR can be adjusted according to a threshold in the specific classifier used in the system. If a threshold is set to a value such that FAR equals FRR, it is called the Equal Error Rate (EER).

The user identification and authentication accuracy for smartphone-based behavioral biometrics can still be increased by improving existing methods (as the research of behavioral biometrics for smartphones is still relatively new) and by discovering new reliable biometrics that can be combined with other biometrics in multi-modal biometric systems.

The behavioral biometrics for smartphones have so far focused primarily on gestures and taps performed on a touch screen and detecting body movements such as walking or simple hand gestures using the accelerometer sensor. One of the body movements that has not been thoroughly examined is the movement of picking up the smartphone on a surface or the user's pocket. Users perform this movement frequently every day, and thus has a great potential as another method of authenticating them seamlessly.

In this paper we determine whether the movement of picking up a phone can serve as another viable biometric for user authentication. We aim to verify this assumption based on an experiment in which 30 participants were tasked to pick up a smartphone from a table upon receiving a fake notification, dismissing the notification and putting the phone back on the table. The experiment was performed with standing and sitting posture and placing the phone on a table and in one of user's front pants pockets, giving four sets of experimental data for each participant.

This rest of this paper is structured as follows. Related work is discussed in Section 2. The proposed method is described in Section 3. Section 4 describes the proposed evaluation of the method. The last Section concludes the work.

2 Related work

Many studies focused on recognizing users based on their gait (walking patterns) using the smartphone's accelerometer [1, 7, 8]. In [8], participants were asked to walk on a flat surface (carpet) up and down a hallway. Before features could be extracted from the accelerometer data, segments related to walking were manually filtered. Features, including x, y and z direction of acceleration and the magnitude of acceleration, were evaluated for each walk segment separately. A similar study [1], also gathering walk data and splitting them into segments, uses raw readings from the accelerometer for x, y and z values and applies wavelet transform on them to gather useful features in time and frequency domains. The study also considers different walking patterns, such as walking in circles or abruptly changing walk direction. These studies ignored data not associated with any of the gait-based activities, including the movements of picking up and placing the phone to a pocket.

Study [9] observed how different positions of a phone affect authentication accuracy for walking users. The results showed that the position of the phone in a hand and in a pocket exhibit different

characteristics and thus may have a significant impact on user authentication accuracy. On the other hand, holding the phone on left or right hand did not affect user authentication accuracy, likewise for having the phone in user's left or right pocket.

Study [3] aims to authenticate users based on the movement performed when answering or placing a phone call, using the smartphone's accelerometer and orientation sensor. The proposed system starts tracking the user once the user presses a button to answer/place a call and brings the phone to the ear. As acknowledged by the authors, this biometric measure can authenticate users transparently as does not require them to perform additional actions in order to train the system. While the accelerometer and the orientation sensor are used to track user's movement, it is unclear from the study how the system recognizes the moment the user brings the phone to the ear (to determine the end of the movement). The proximity sensor, commonly found in smartphones, could be used as an indicator that the user is holding the phone to the ear.

The movement of picking up and placing the phone was also subject to research [4–6, 13]. In general, accelerometer is used to gather raw data, along with gyroscope and magnetometer in several studies. In [4], participants were asked to pick up the phone from a table in two different postures – sitting and standing. In [5], the gathered data were split into three phases – picking up the phone from a table, holding the phone to the ear and placing the phone back on the table.

While the movement trajectories were already studied in [4], it is assumed that the start and end of these movements (picking up the phone, dismissing the notification, placing the phone) exhibit unique movement patterns for each user.

Compared to previous studies, this paper evaluates the movement in multiple postures – sitting and standing – and in different places of the phone – a table and user's front pants pocket. Additionally, the method takes the application context taken into account to determine the start of the movement, making the method applicable in real-world scenarios.

3 Method

This Section describes the proposed method to authenticate users based on the movement of picking up a smartphone from a table and one of user's pockets.

Users receive notifications on a daily basis - SMS messages, calendar reminders, e-mails or phone calls. From the moment user picks up the phone, the application logs data from the accelerometer sensor until the user explicitly dismisses the notification.

Using the sensors should be kept to a minimum to avoid excessive resource usage (especially on mobile devices), including battery power. Therefore, it is strongly recommended that the sensor data be logged only from the time to pick up the phone until the user dismisses the notification (reads a message, postpones a reminder, accepts the phone call).

3.1 Features

The following proposed features are extracted from the raw accelerometer readings:

- minimum, maximum, mean and standard deviation of acceleration for x-, y-, z-acceleration and magnitude of acceleration (computed as $m = \sqrt{x^2 + y^2 + z^2}$), respectively,

- pick-up time – time from receiving a notification until its dismissal.

The features discussed are computed for each pick-up movement separately, starting with the moment a notification is generated and ending when the accelerometer readings show that the phone is no longer being moved, or a specified number of seconds after the dismissal if the phone is still being moved. It is yet to be determined how many seconds in the latter situation is optimal for each examined posture.

The pick-up time may not always be a reliable feature in real-world scenarios. For example, the length of a received message may delay the user dismissing the notification. For the controlled experiment described later in this paper, the displayed messages are short enough to not delay the user for too long.

3.2 Matching users

Once computed, the features form a vector of values to act as an input to a classifier. In this paper, we choose the k-Nearest Neighbors (k-NN) algorithm and the Support Vector Machine (SVM) due to their good classification performance. SVM as a binary classifier is convenient for user authentication as the features for the phone owner can be treated as one class of data and features for non-owners (impostors) as another class.

In practice, however, it is unusual for a smartphone to be used by more than one person. A biometric system therefore has no plausible way to gather enough data from non-owners. Given this limitation, one-class SVM [12] is used as another classifier to determine whether the extracted features closely match the phone owner's.

Given that accelerometer readings can be represented as time series, the readings can be compared with each other in terms of their similarity to identify or authenticate users. For this purpose, the Dynamic Time Warping (DTW) algorithm is used as another user matching method to compare against k-NN and SVM.

4 Evaluation

This Section describes the evaluation of proposed method in the Section 3. The method is verified based on a controlled pilot experiment.

4.1 Experiment description

30 users in total participated in the experiment composing of four simple tasks. In the first task, the participants were instructed to sit down on a chair in front of a table. The participant first places a phone on the table. After a small period of time, the phone vibrates and generates a notification (an SMS message or a calendar reminder with sample text), the participant picks up the phone, reads and dismisses the notification and places the phone back on the table.

Each task is performed four times in total in order to generate a sufficient amount of sample data for each user without unnecessarily prolonging the experiment. In real-world scenarios, the number of samples should be much higher (at least in tens) to provide good accuracy of classifiers used for this method.

In the subsequent tasks, the participant is instructed to stand up and repeat the task, then repeat the same task while sitting and placing the phone in the front pants pocket and finally while standing and placing the phone in the front pants pocket. Figure 1 shows a sample of raw accelerometer readings for a pick-up movement from a table while a user is sitting. The first two valleys represent the phone vibration as a result of a generated notification. The subsequent readings show the user picking up the phone, reading the notification, dismissing the notification and putting the phone back on the table.

It is apparent that phone vibrations are undesirable and that this segment must be filtered prior to extracting features. Simply removing the segment containing phone vibration is not a viable solution because the user may pick up the phone while the phone is vibrating. It is yet to be determined whether phone vibrations can be safely filtered in the frequency domain without accidentally filtering the useful data. As an alternative, if it is known which vibration pattern corresponds to which notification, we may be able to build different user templates for different types of notifications without filtering the vibration patterns. Each user performed the experiment with the same phone, *HTC Desire* with Android operating system (version 2.2). Apart from the accelerometer sensor,

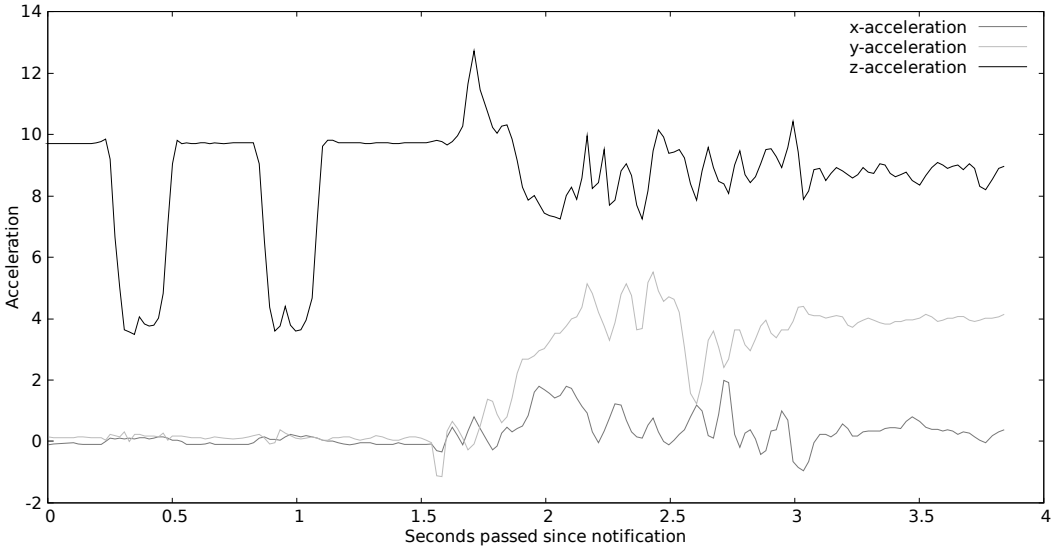

Figure 1. Raw accelerometer readings for a pick-up movement from a table for the sitting posture.

other sensors were recorded as well, including the magnetometer and touch screen, reserved for further evaluation of the method in the future. The data were logged continuously during the entire experiment for each user individually. Each action (start of task, notification generated, notification dismissed) was associated with a time stamp to help identify segments belonging to the pick-up movements. The labeled segments also help identify each task with different postures and phone positions to treat each task separately during the evaluation.

There are several real-world factors not considered in the experiment that could affect users' movement patterns, such as table height, distance of the phone from the user, different pocket size or users having no pockets at all. Users may react differently given the application context, such as receiving a message, a reminder or a phone call.

Users may pick up the phone with either the left or right hand, causing the trajectories to differ. Given the conclusions in [9] for walking movements, it is expected that picking up or placing the phone with the left or right hand will not impact user authentication accuracy.

4.2 Evaluation of results

To evaluate the performance of the proposed method for one user, we set the user as the phone owner and other users as non-owners. The classifier then determines the false positive rate and false negative rate, considered to be FAR and FRR, respectively. Once the performance is evaluated for each user, we compute the mean FAR and FRR for all values of FAR and FRR from each user, which finally represents the accuracy of the proposed method for user authentication.

It is expected that the extracted features will differ for different postures (standing, sitting) and different phone positions (table, pocket) for the same user. The authentication performance is therefore evaluated for the following combinations:

- postures and positions individually,
- all postures combined,
- all positions combined,

– all postures and positions combined.

Likewise, the performance of classifiers specified in Section 3.2 is compared.

5 Conclusions and future work

This paper proposes a method to authenticate users based on how they pick up smartphones from a flat surface (a table) or their front pants pockets. The goal of the pilot experiment is to determine whether the movement of picking up a smartphone can be used to distinguish users and can thus be used as another viable behavioral biometric characteristic. Additionally, the contribution of this paper is to determine how different postures and phone positions affect the user authentication accuracy for this type of movement.

The future work comprises actual evaluation, including using the DTW algorithm on accelerometer readings and gathering features from additional data logged during the experiment - touch screen data and magnetometer readings. To match the pick-up time closer to the real-world scenarios, it may be redefined as the time the user picks up the phone until the phone stops moving - that is, until the phone's accelerometer readings become stable for a specific time period.

Beside the pick-up movement, placing a smartphone back on the table or users' pockets will also be examined as it may exhibit unique biometric characteristics. In this case, however, we cannot precisely determine when the user stops placing a phone as the user performs no explicit action afterwards. Given the accelerometer sensor, we may be able to detect if the phone stops moving as per the redefinition of the pick-up time feature.

Given that in the pilot experiment we also recorded additional sensors, such as magnetometer and touch screen, we are able to compute additional features that may improve the performance of the method, such as velocity-related features, phone's orientation or pressure applied on touch screen (which proved to vastly improve the accuracy of user authentication in related works [2, 10, 11]).

The movement of picking up a phone can further be divided to three segments – start of motion (grabbing the phone), motion proper (drawing the phone closer to user's body) and end of motion (the phone stops moving) – as each of these segments exhibits vastly different values, especially in terms of phone's acceleration.

Acknowledgement: This work was partially supported by the Scientific Grant Agency of Slovak Republic, grant No. VG 1/0774/16.

References

[1] Boyle, M., Klausner, A., Starobinski, D., Trachtenberg, A., Wu, H.: Gait-based User Classification Using Phone Sensors. In: *Proceedings of Conference on Mobile Systems, Applications and Services*.

[2] Chang, T.Y., Tsai, C.J., Lin, J.H.: A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices, vol. 85, no. 5, pp. 1157–1165.

[3] Conti, M., Zachia-Zlatea, I., Crispo, B.: Mind How You Answer Me!: Transparently Authenticating the User of a Smartphone when Answering or Placing a Call. In: *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*. ASIACCS '11, ACM, pp. 249–259.

[4] Feng, T., Zhao, X., Shi, W.: Investigating Mobile Device Picking-up motion as a novel biometric modality. In: *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, pp. 1–6.

[5] Kunnathu, N.: Biometric User Authentication on Smartphone Accelerometer Sensor Data.

[6] Makaram, Y.: The Phoney Lift: Using Accelerometers to Identify People.

[7] Nickel, C., Derawi, M., Bours, P., Busch, C.: Scenario test of accelerometer-based biometric gait recognition. In: *2011 Third International Workshop on Security and Communication Networks (IWSCN)*, pp. 15–21.

[8] Nickel, C., Wirtl, T., Busch, C.: Authentication of Smartphone Users Based on the Way They Walk Using k-NN Algorithm. In: *2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, pp. 16–20.

[9] Primo, A., Phoha, V., Kumar, R., Serwadda, A.: Context-Aware Active Authentication Using Smartphone Accelerometer Measurements. In: *2014 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pp. 98–105.

[10] Saevanee, H., Bhatarakosol, P.: User Authentication Using Combination of Behavioral Biometrics over the Touchpad Acting Like Touch Screen of Mobile Device. In: *International Conference on Computer and Electrical Engineering, 2008. ICCEE 2008*, pp. 82–86.

[11] Saevanee, H., Bhattarakosol, P.: Authenticating User Using Keystroke Dynamics and Finger Pressure. In: *6th IEEE Consumer Communications and Networking Conference, 2009. CCNC 2009*, pp. 1–2.

[12] Schölkopf, B., Williamson, R.C., Smola, A.J., Shawe-Taylor, J., Platt, J.C.: Support Vector Method for Novelty Detection, vol. 12, pp. 582–588.

[13] Shrestha, B., Mohamed, M., Borg, A., Saxena, N., Tamrakar, S.: Curbing mobile malware based on user-transparent hand movements. In: *2015 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 221–229.

[14] Zheng, N., Bai, K., Huang, H., Wang, H.: You Are How You Touch: User Verification on Smartphones via Tapping Behaviors. In: *2014 IEEE 22nd International Conference on Network Protocols (ICNP)*, pp. 221–232.