Information Sciences 430–431 (2018) 538–553

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Performance evaluation of implicit smartphones authentication via sensor-behavior analysis

Chao Shen*, Yufei Chen, Xiaohong Guan

Xi'an Jiao Tong University, No.28 Xianning West Road, Xi'an 710049, China

ARTICLE INFO

Article history:
Received 9 September 2017
Revised 12 November 2017
Accepted 29 November 2017
Available online 5 December 2017

Keywords:
Smartphone security
Motion sensors
Biometric authentication
Performance evaluation

ABSTRACT

The pervasiveness of mobile devices not only facilitates people's daily life with a wide variety of services, but also brings users risks of private information leakage (e.g., photos, contact lists, bank accounts), which emphasizes the demand for reliable, feasible and user-friendly authentication mechanisms on mobile devices. In this paper, we develop an authentication mechanism using motion sensors (accelerometer and gyroscope) embedded in smartphones. Our proposed mechanism performs authentication continuously and implicitly by monitoring the user daily activities. We extract time-, frequency- and wavelet-domain features from motion-sensor data, and conduct empirical feature analysis to investigate the optimal combination of features, to acquire a fine-grained characterization of users' movement patterns. To make a systematic performance evaluation, we have established a dataset containing 27,681 samples, including five kinds of actions and five different smartphone placements. In the evaluation procedure, four kinds of contexts are considered (nothing-aware context, action-aware context, placement-aware context and full-information-aware context), and ten one-class detectors are implemented. The best accuracy (represented as *EER*) for the four conditions achieves 28.22%, 2.21%, 5.50% and 3.28%, respectively, indicating our proposed approach is feasible and applicable in some real scenarios. Moreover, the performance analyses for sensor combinations and feature combinations are also conducted.

1. Introduction

With significant promotion in computing, sensing and network, the smartphone becomes a ubiquitous and popular platform providing various online services, such as email, online shopping, personal communication and etc. However, as smartphones provide people with more convenient services, in the meanwhile, they also expose sensitive personal information (e.g., photos, contact lists, bank accounts) to potential attackers. It is necessary to explore a more reliable and secure approach for user authentication.

PIN codes and passwords are the most commonly used in authentication mechanisms. However, people tend to use weak passwords since short or simple passwords are easy to remember and input, which will increase the risk of information disclosure in the meantime. Unfortunately, even if complex passwords are applied, they can also be derived by detecting the location of screen taps based on accelerometer and gyroscope readings [21]. One possible way to solve this

* Corresponding author.
E-mail addresses: cshen@sei.xjtu.edu.cn, chaoshen@mail.xjtu.edu.cn (C. Shen).

https://doi.org/10.1016/j.ins.2017.11.058

problem, considering both usability and security, is implementing the continuous authentication based on biometric features. Such continuous authentication does not rely on the direct involvement of the user, but is closely related to his/her biometric behavior, habits or living environment [14]. And moreover, it continuously monitors the user's identity rather than only authenticates once at the entry point, so it is capable of enhancing the system security. In early studies, the main topic focused on video-based authentication mechanisms (e.g., gait [7], face [33]). In these years, with the big advance in MEMS (micro-electro-mechanical systems), mobile devices equipped with motion sensors (accelerometer, gyroscope, etc.) have been widely used. In that case, a new branch in the biometric authentication field has emerged. A lot of literature call this mechanism *sensor-based authentication*, which implements authentication via the data provided by physical devices attached to the body (e.g., from motion sensors [1,18]), or data generated during the human-machine interaction (e.g., from touchscreen [25,29]).

While the touch behavior only exists in the human-machine interaction, the motion behavior exits throughout the whole phone use process, even when the phone is locked. That is, the motion-sensor-based authentication can provide longer security monitoring. In the motion-sensor-based authentication field, the experimental contexts are complex: Firstly, diverse sensors are applied. The most commonly used sensor is accelerometer [9,13,20,22,23,32], while other sensors like gyroscope [19,31] and orientation sensor [5,14] are also employed; secondly, different actions are performed, for example, walking [9,20,32], shaking the phone [22], jogging, descending and ascending stairs [13]; thirdly, the positions which devices are attached to are various, including hand-held [22], pockets [13,31], hip [9], and waist [31].

However, despite studies conducted in a wide variety of experimental scenarios, there are a few full-scale studies about authentication in multiple contexts. Although some work has evaluated how the placements affect the activity recognition [3,28], in the sensor-based authentication field, to the best of our knowledge, there is little work about how the actions or the sensor placements affect the performance.

This paper represents an investigation in some factors which may impact the authentication performance. Five actions (descending stairs, ascending stairs, walking, jogging and jumping) and five placements (right upper arm, right hand, right jacket pocket, right trousers pocket and waist.) are included in our experiments to make a systematic performance evaluation. Then we make a brief analysis of the results and attempt to give some advice on how to improve the authentication performance. This paper aims to answer the following questions:

- How do the actions and placements affect the performance?
- Which features are effective to distinguish different users?
- Which classification algorithms perform better in the authentication stage?
- How to improve the authentication performance?

In this paper, we represent a continuous and implicit smartphone authentication system via motion sensors embedded in the phone, which discriminate the users by analyzing motion data generated in human daily activities, and show a systematic performance evaluation on various factors. First, we collect the data from inertial sensors with a third-party data acquisition application (running as a background process), and conduct the data preprocessing to filter the noise and segment the long-lasting data. Second, we extract time-, frequency- and wavelet-domain features for fine-grained characterization of user identity. Third, we apply a nonparametric test to each dimension of original feature vectors to examine the feature discrimination between different subjects, and according to the analysis of the test result, we perform a feature selection and build up the final feature vector. And then, we implement ten one-class classifiers to compare their performance. To get a full-scale evaluation, we asked ten volunteers to behave five basic actions: descending stairs, ascending stairs, walking, jogging and jumping. What's more, during the procedure of data collection, we placed the smartphone at five different positions: right upper arm, right hand, right jacket pocket, right trousers pocket and waist. Finally, we established a dataset consisting of 27,681 activity samples. Then, we conduct the evaluation in *nothing-aware context* (neither the action nor the placement was informed), *action-aware context* (the corresponding action was informed), *placement-aware context* (the corresponding placement was informed), and *full-information-aware context* (both the action and placement were informed). Ten detectors are implemented in our study, and for the four contexts, the Mahalanobis distance-based detectors showed an outstanding performance compared with others, whose lowest EER achieved 28.22%, 2.21%, 5.50% and 3.28% respectively. Our results show that our proposed authentication mechanism is feasible and reliable in some cases. Furthermore, to facilitate further study, we evaluate authentication performance with different combinations of sensors and features.

The main contributions of this paper are as follows:

- To make a more comprehensive evaluation, we established a dataset with 27,681 samples from ten participants including action data with typical actions and phone placements. During the collection procedure, we required the participants to perform five different actions (descending stairs, ascending stairs, walking, jogging and jumping), and we chose five different positions to place the smartphone (right hand, right top arm, right jacket pocket, right hip pocket and waist). Then we evaluate the influences of actions and smartphone placements.
- We make a brief summary of multiple features (time-, frequency-, wavelet domain) from action-recognition literature, and employ them to our study, so that we can exploit more implicit information behind peoples actions.
- We apply a nonparametric test to analyze the feature discrimination statistically, and the results enable us to discover what attributes mainly reflect the differences among different individuals, and then help us to implement feature reduction.