Mobiles and Wearables: Owner Biometrics and Authentication

Kamen Kanev
Faculty of Informatics
Shizuoka University
+81 53 478 1326
kanev@rie.shizuoka.ac.jp

Maria De Marsico
Department of Computer Science
Sapienza University of Rome
+39 06 49918312
{demarsico, bottoni, mecca}@di.uniroma1.it

Paolo Bottoni
+39 06 4925 5166

Alessio Mecca
+39 06 49918312

ABSTRACT
We discuss the design and development of HCI models for authentication based on gait and gesture that can be supported by mobile and wearable equipment. The paper proposes to use such biometric behavioral traits for partially transparent and continuous authentication by means of behavioral patterns.

CCS Concepts
• **Security and privacy~Biometrics** • *Human-centered computing~Activity centered design*

Keywords
User identification; transparent authentication; continuous biometric input; mobile motion tracking; wearable monitoring.

1. INTRODUCTION
Human computer interaction (HCI) has been an essential part of everyday life for quite a while and we have already reached the point when we do not even notice it, especially when it comes to mobile devices like smart phones and wearables. We see the ubiquitous computing facilities that saturate the modern world mostly as means for obtaining different services and natural support during our activities. There is a need, therefore, to make traditional HCI models evolve and to shape them for better consideration of new interaction modalities. In particular, user authentication is an operational need for secure ubiquitous access to services and functionalities. We discuss here the design and development of HCI user authentication models for mobile and wearable devices and equipment. Since such devices are typically owned individually, hence highly personalized, we pay special attention to continuous user and owner identification coupled with transparent authentication during their normal use.

2. TRANSPARENCY AND CONTINUITY IN MOBILE USER AUTHENTICATION
User authentication is *transparent* when no interaction facilities and actions specifically engaging the user are employed. An example would be unlocking a fingerprint lock-enabled smartphone by pressing its `Home` button. Conversely, requesting a user to present its finger for scanning with a fingerprint reader at a door lock or at an ATM would constitute an example of non-transparent user authentication. Authentication is *continuous* when it is not implemented as a single step but is essentially iterated along with the interaction. Obviously, unlocking a smartphone by presenting a registered fingerprint is non-continuous. A good example of continuous and transparent authentication could be employing a mouse with an embedded fingerprint scanner in a traditional desktop environment (see e.g. [1,2], where wearable RFID rings for user identification were also employed). Transparent *and* continuous user (re-)identification is not always possible. For example, recognition from gait can be carried out transparently and partially continuously by wearable accelerometers, while recognizing a person from password entails some voluntary action.

Authentication to a service always implies a kind of preliminary enrollment phase, e.g., the user chooses a username and a password, or provides his/her fingerprints to create a biometric template to match in the following access phases. In order to gain access to the service, the user claims his/her identity (e.g., through the username) and this identity must be verified e.g., using the password or the fingerprint or both. In biometric research, this modality is defined as verification, and entails 1:1 matching with the enrolled template of the claimed identity. Without the preliminary identity claim, matching must be carried out against all possibly enrolled users, therefore entailing a much heavier 1:N comparison, technically defined as identification. In the case of mobile devices and wearables, the authentication process can be simplified and optimized in different ways. We can assume that such equipment is used exclusively by its owner (implicit identity claim), or previously allow its unlocking by a further verification step carried out on the device itself, as quite usual nowadays on smartphones. In this way, the service can be granted to the rightful user by only verifying again upon access request. Note that even nowadays users are often required to identify themselves by entering user names and IDs, by employing magnetic and/or RFID cards, deliberately presented to a receiver, or by other explicit means. Even fingerprint-enabled door locks usually require PIN codes that essentially function as registered user IDs, impairing their naturalness. Eliminating the need to identify the user makes a big difference for the design of the HCI model and interaction functionalities. Such a difference becomes particularly important for mobile and wearable devices with limited computing power.

3. MOBILE USER BIOMETRICS
Present technologies allow continuous monitoring of human body parameters such as pulse, blood oxygen and pressure, temperature, etc., via wearable devices. Hence, one can envisage different interaction models for devices with such integrated human monitoring capabilities. Wearables connected by Bluetooth to a Smartphone can serve, e.g., as a secure, always

AVI '16, June 07-10, 2016, Bari, Italy.
ACM 978-1-4503-4131-8/16/06.
http://dx.doi.org/10.1145/2909132.2926084

on, biometric authenticator. In fact, many recent works focus on ECG-based authentication with a low number of electrodes.

As for security, however, much research is still needed to demonstrate the reliability of authentication based solely on standard biometric information gathered by currently available wrist-wearables. Moreover, even a fingerprint reader embedded in current smartphones appears to be fairly easy to circumvent by fingerprint lifting and reproduction [3]. Major concerns lie, therefore, with possible lack of sufficient user authentication reliability and the dangers of identity forging in the second case.

We address the above concerns by considering methods for biometric identification that are not based on *what humans are*, e.g. biometrics that can be forged, but rather on *the way humans behave*. Users are engaging in specific behavioral patterns every time they employ a mobile or a wearable device to obtain access to a service or a support. Our idea is to utilize such behavioral patterns for transparent and continuous authentication.

4. PRELIMINARY EXPERIMENTS

4.1 Gait

Part of our recent work is dealing with an approach to gait recognition based on a single consumer accelerometer, built in most present mobile devices. In particular, better ways to exploit the Dynamic Time Warping (DTW) are being investigated, since this algorithm is still one of the most used at present in literature. Both a new step segmentation algorithm to split the gait signal into cycles/steps, and matching strategies to compare the possibly segmented signal for recognition are the main topics of this part of the research. We have carried out many tests on three different datasets, collected using different sensors. The best result in identification was achieved using the most constrained method, i.e., limiting the walks to have a similar number of steps. It reaches about 93% of Recognition Rate (RR – rate of tests where the right subject is returned as the first in a candidate list). The best result with methods exploiting segmentation to overcome the mentioned limitation reaches about 83% of RR on the same dataset. The best result in verification is achieved with an Equal Error Rate (EER) of 0.09, while the best result with segmentation is an EER of 0.10. This is a very good result for a soft biometrics as gait is often considered. More details can be found in [4].

4.2 Spatial Handwriting

As discussed in section 4.1, motion tracking information continuously gathered by a mobile device while carried by its owner can be used for transparent biometric authentication. Since the user is being continuously authenticated while on the move, an incoming phone call, for example, can be received safely, without the need to explicitly unlock the phone. While continuous user authentication could be extended to motion patterns associated with different other activities, in some cases gathered motion data might be insufficient for reliable biometric authentication. We address this issue by considering natural hand gestures. The goal is to recognize people through gestures instead of recognizing gestures made by different people. As usual in biometrics, the authentication process entails a preliminary enrollment. During this phase, the user should choose and make a gesture in the air with the hand holding the device embedding the accelerometer. Of course, such 3D hand gesture must be repeatable by the user, at the same extent of a handwritten signature, and can be used as his/her identifying template. During the access phase, the user must repeat the chosen identifying 3D gesture to access the system. In some sense, the chosen gesture represents a password, while the way to perform it is a further identifying dynamic user feature. Although different sets of gestures could be used for this purpose [5], we focus here on handwriting and sign gestures [6]. In Japan, the writing system is based on two alphabets and a set of over 2000 Kanji characters. Japanese names are typically written in Kanji and there are different ways to write the same name. On many occasions, Japanese would illustrate their names by "handwriting in the air", which we recognize as a natural communication paradigm widely accepted in Japan. We have thus designed and developed an HCI framework for biometric user identification, with preliminary results discussed in [6]. In our experiments, we employed 5 different elementary gestures matched to appropriate Kanji strokes. Based on them 10 Kanji characters each comprising of 2 to 7 strokes were constructed and drawn in the air by 17 different users. The corresponding motion data was collected by an Android Smartphone, processed, stroke sequenced, and analyzed. After some user training, the highest recognition rate went slightly over 96% for horizontal strokes and reached 100% for 2 of the Kanji characters in the set.

5. CONCLUSIONS

Biometric behavioral traits are more difficult to forge, generally allowing for transparent and continuous recognition. However, they are considered as soft traits, providing less reliable recognition than e.g., fingerprints. This is mainly due to both external and personal factors, e.g., a cold alters voice, the shape of the ground can affect gait, etc. This limitation can be overcome by adopting a multi-biometric approach. In this work, we have sketched a proposal implying the use, either in parallel or in different times, of gait and handwriting in the air. Both biometrics can be acquired and processed by mobile devices, and therefore can support ubiquitous and natural interaction.

6. ACKNOWLEDGMENTS

This work was supported in part by funding for exchange of researchers provided by the Ministry of Foreign Affairs of Italy.

7. REFERENCES

[1] Kanev, K., Kamiya, N., Mirenkov, N., Kanda, G., Takagi, A., Adaptive E-learning Applications with Transparent User Identification, In *Proc HC'07*, 13-15, 2007, pp. 25-30.

[2] Kanev, K., Kimura, S., Collaborative Learning in Dynamic Group Environments, Book chapter in "Distance Education Environments and Emerging Software Systems: new Technologies", Qun Jin (Ed.), IGI Global, 2011, pp.1-14.

[3] J. Galbally-Herrero, J. Fierrez-Aguilar, J. D. Rodriguez-gonzalez, F. Alonso-Fernandez, J. Ortega-Garcia and M. Tapiador, "On the Vulnerability of Fingerprint Verification Systems to Fake Fingerprints Attacks," Proc. ICCST'06, pp. 130-136, IEEE, 2006.

[4] De Marsico, M., & Mecca, A. (2015, September). Biometric Walk Recognizer. In *Proc.-ICIAP 2015 Workshops* (pp. 19-26). Springer International Publishing.

[5] Guerra-Casanova, J., Sánchez-Ávila, C., Bailador, G., & de Santos Sierra, A. (2012). Authentication in mobile devices through hand gesture recognition. *International Journal of Information Security*, *11*(2), 65-83.

[6] Kanev, K., De Marsico, M., Bottoni, P., A Human Computer Interactions Framework for Biometric User Identification, *Jap. Journal of Applied Physics Conf. Proc.*, Vol. 4, 2016, 011601(1-6).