

Bachelorprojekt

Seminar Title (e.g., Geographic Visualizations)

SoSe 2020

Johannes Waltmann

University of Duisburg-Essen
Matrikulationsnummer: 3029975
`johannes.waltmann@stud.uni-due.de`

Abstract. The abstract should briefly summarize the contents of the work in 150–250 words. Can I quote here?

1 Introduction

During the last years the usage of smart-wearables (particularly smartwatches) has become more and more common with a number of 337 million units sold in 2019 and a forecast in sales of up to 527 million units by 2024 [1]. With that also comes a natural demand in data protection due to the many sensors built in these devices due to their ability to capture sensible personal information (e.g. health informations) and additionally the fact that smart devices also can now be used for many kinds of financial actions.

Since most wearables are connected to either the distributors or the respective mobile phones virtual assistant they should contain sensors for on one hand sound conduction and on the other hand audio recording.

Based on these conditions smartwatches could be used in combination with biometric authentication mechanics.

In general biometric authentication can be split into behavioural and physiological biometrics as well as authentication can be split into implicit and explicit methods. The exact characteristics will be described as follows:

1.1 Biometrics

Biometrics (as in the greek terms *bios* and *metrikos*) describes the utilization of an individuals physical traits or behaviour to clearly identify one from others. Contrary to the more known verification methods as PINs, passwords or ID-cards biometric identification does not rely on tokens or knowledge which could easily be forgotten or stolen, rather than unique personal traits like fingerprints, face or the specific way someone interacts [5, chpt. 1.1][3]. Therefore the individual wishing to authenticate first has to enrol one specific trait of hers to the biometric system. Based on this sample data the system generates an authentication template which is later on used to authenticate against.

When someone now wants to register using the system he provides the trait wanted to the system from which then a new sample is generated. The generated sample then is compared to the template [2].

Tests used for this comparison can be designed based on two different points of view. First of positive identification or authentication and second negative identification/authentication. Negative authentication presumes the given sample is from an unknown user whereas the sample in a positive authentication scenario should be by a known user [10]. As already stated above biometric authentication uses an individuals personal traits as authentication tokens. Based on the kind of trait and the methods how they could be provided the general term of biometrics can be further divided into *behavioural* and *physiological* biometrics. How each of them is defined exactly will be defined in the following.

Behavioural Biometrics Behavioural biometrics refers to authentication systems in which process of authentication is conducted with the use of primarily gestures or other actions able to be performed in everyday life. Usable features for this purpose are e.g. gait or keystroke analysis. Advantages this kind of biometrics has are e.g. that there is no direct need for special hardware since it is mostly used with smart wearables or mobile phones who each have the required sensors built in. Another advantage would be that the data required must not be collected actively by the user but is recorded passively by the sensors of the used smart device [11].

Physiological Biometrics Apart from behavioural biometrics there is also the classification of physiological biometrics. This form of biometric authentication uses the more "static" traits of a users body as tokens such as e.g. fingerprints, hand geometry, vein patterns [2], [4]. A physiological system should also have a little higher accuracy than a behavioural one and it should be harder to use as an imposter since it is nearly impossible to identically copy a finger print, iris pattern, etc. [6], [3].

1.2 Authentication

A further subdivision which can be made in the context of authentication is between explicit and implicit authentication. By *explicit* authentication one understands interactions with a security system which are performed actively. This includes providing knowledge like PIN or password, using a token but also performing gestures, fingerprints etc. from the biometrical field.

Work presented by Shi et al. states that *implicit* authentication would be a perfect fit for usage in combination with mobile devices [9]. Since users are using their devices on slightly different habits everyday the data collected by built-in sensors alternates between individuals but stays the same for one person. Exploiting this they propose three application scenarios for the use of implicit authentication.

First as a second factor in combination with passwords, second as the main authenticator and thus replacing the usage of a password and last as additional assurance or an extra trust factor when performing financial actions on a mobile device.

Grob: Was gemacht und welche (major) Ergebnisse

2 Related Work

Major influence towards this work comes from Schneegaß et al. works on functional biometrics as a novel kind of biometric authentication [7] and one of its first realizations with SkullConduct [8]. These and other works on smart device based biometric authentication will be described in this section.

As mentioned above Schneegaß et al. introduced a novel kind of biometrics named *functional biometrics*. This category subordinates to physiological biometrics since its key feature is the usage of body reflections.

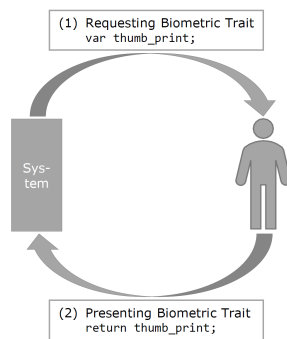


Figure 1. Authentication request performed by a "traditional" biometric system

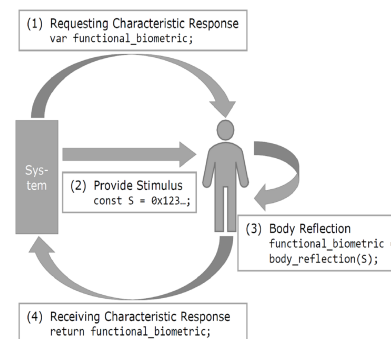


Figure 2. Authentication request when performed by a system using functional biometrics

With functional biometrics the authentication system provides an additional stimulus during the enrolment phase. This stimulus is applied to the individuals body where it gets modified and afterwards captured (Figure 2). Due to different personal biological characteristics the modification of the stimulus is unique for each combination of user and stimulus.

Requirements Schneegaß et al. proposed are two hardware components in form of a Stimulus Generation Unit (SGU) and a Body Reflection Sensor (BRS). These two have to be designed as a dependence of the underlying biometric trait. Exemplarily when sound is used as the stimulus the SGU will be most likely some kind of microphone and the BRS a speaker.

During the enrolment process described above stimulus and its transformation are saved as a secret two-tuple $(x, f(x))$ with x being the stimulus and $f(x)$ the transformation. Now when the related user wants to authenticate the stimulus is reapplied and it is expected to get $f(x)$ as response again. An additional security measure provided by functional biometrics is that when the stimulus gets leaked or lost the system is not fully compromised because the stimulus is only an exchangeable medium. The secret stems from the body reflection function which is unique to the user, unknown and hard to manipulate.

(Hier Skullconduct und 1, 2 andere Smart Wearable Authentication Works)

3 Concept

4 Implementation

5 Evaluation

6 Conclusion

first level: section

second level: subsection

third level: subsubsection

fourth level: paragraph

Table 1. Table captions should be placed above the tables.

Heading level	Example	Font size and style
Title (centered)	Lecture Notes	14 point, bold
1st-level heading	1 Introduction	12 point, bold
2nd-level heading	2.1 Printing Area	10 point, bold
3rd-level heading	Run-in Heading in Bold. Text follows	10 point, bold
4th-level heading	<i>Lowest Level Heading.</i> Text follows	10 point, italic

Displayed equations are centered and set on a separate line.

$$x + y = z \tag{1}$$

Please try to avoid rasterized images for line-art diagrams and schemas. Whenever possible, use vector graphics instead (see Figure 3).

References

1. Themenseite: Wearables, <https://de.statista.com/themen/3471/wearables/>

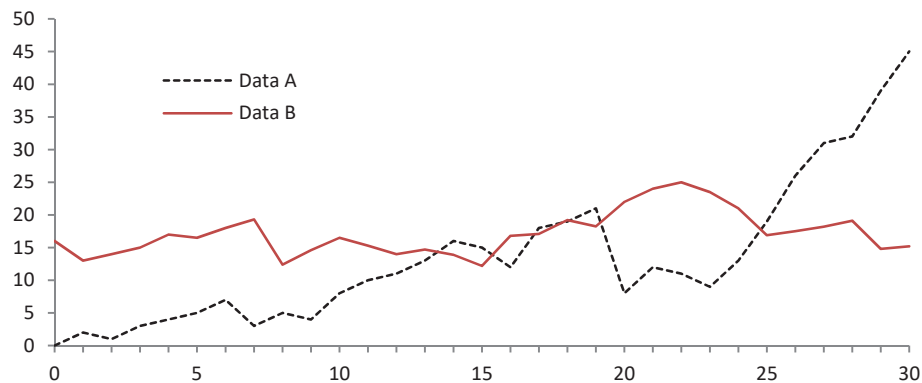


Figure 3. A figure caption is always placed below the illustration. Please note that short captions are centered, while long ones are justified by the macro package automatically.

2. Alsaadi, I.M.: Physiological biometric authentication systems, advantages, disadvantages and future development: a review. *international journal of scientific & technology research* **4**(12), 285–289 (2015)
3. Delac, K., Grgic, M.: A survey of biometric recognition methods. In: *Proceedings. Elmar-2004. 46th International Symposium on Electronics in Marine*. pp. 184–193. IEEE (2004)
4. Faltaous, S., Liebers, J., Abdelrahman, Y., Alt, F., Schneegass, S.: Vpid: Towards vein pattern identification using thermal imaging. *i-com* **18**(3), 259–270 (2019)
5. Jain, A.K., Flynn, P., Ross, A.A.: *Handbook of biometrics*. Springer Science & Business Media (2007)
6. Koong, C.S., Yang, T.I., Tseng, C.C.: A user authentication scheme using physiological and behavioral biometrics for multitouch devices. *The Scientific World Journal* **2014** (2014)
7. Schneegass, S., Liebers, J.: Introducing functional biometrics: Using body-reflections as a novel class of biometric authentication systems. In: *Proceedings of the 2020 CHI Conference* (2020)
8. Schneegass, S., Oualil, Y., Bulling, A.: Skullconduct: Biometric user identification on eyewear computers using bone conduction through the skull. In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. p. 1379–1384. CHI '16, Association for Computing Machinery, New York, NY, USA (2016). <https://doi.org/10.1145/2858036.2858152>
9. Shi, E., Niu, Y., Jakobsson, M., Chow, R.: Implicit authentication through learning user behavior. In: *International Conference on Information Security*. pp. 99–113. Springer (2010)
10. Wayman, J., Jain, A., Maltoni, D., Maio, D.: An introduction to biometric authentication systems. In: *Biometric Systems*, pp. 1–20. Springer (2005)
11. Yampolskiy, R.V., Govindaraju, V.: Behavioural biometrics: a survey and classification. *International Journal of Biometrics* **1**(1), 81–113 (2008)