Bachelorprojekt
Title
SoSe 2020

Johannes Waltmann

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

Abstract. tbd

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.
Previous works in this field exploited amongst others gyro- and acceleration-sensors for the purpose of authentication [6], [14]. Based on these results it is arguable that there is room for smartwatch based authentication. Also with the presentation of a novel kind of biometrics named *functional biometrics* the use of smart wearables as a medium for implicit and passive authentication rises.
Focussing on these new techniques this work introduces a prototype for smartwatch based authentication using body conduction of sound. This prototype can be classified in the category of functional biometrics. It uses a microcontroller equipped with a microphone and speaker to generate and capture an audio sample.

2 Related Work

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:

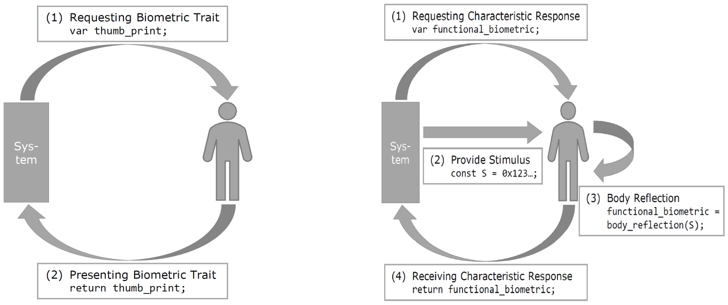
2.1 Biometrics

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 [12]. 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 [13].

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. [7], [3].

Functional Biometrics With functional biometrics another novel kind of biometric authentication was introduced lately by Schneegass et al. [9]. This new


(1) Requesting Biometric Trait
var thumb_print;
Sys-
tem
(2) Presenting Biometric Trait
return thumb_print;
(1) Requesting Characteristic Response
var functional_biometric;
Sys-
tem
(2) Provide Stimulus
const S = 0x123…;
(3) Body Reflection
functional_biometric =
body_reflection(S);
(4) Receiving Characteristic Response
return functional_biometric;

(a) Traditional Biometrics (b) Functional Biometrics

Figure 1. Fig. 1a shows the authentication process of a traditional biometric system. Fig. 1b shows the order of steps for functional biometrics when a stimulus is added [9].

concept stands as a major influence to this work notably with its first implementation in SkullConduct[10].
In this category of biometric authentication 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 1b). 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.

2.2 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 [11]. 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.

As already mentioned before the SkullConduct work by Schneegass et al. is one of the key influences to this work. Not just because it is one of the first realizations for functional biometrics but it also serves as a source of inspiration for this work. Schneegass et al. implemented a biometric authentication system using eyewear computers (e.g. Google Glass). Therefore they used the concept of bone conduction which is already frequently used by hearing aids. SkullConduct, in this case, uses the bone conduction speaker of the Google Glass to emit a sound sample against the wearers head. The sample which gets transformed due to the unique nature of each individuals head is captured by the glasses integrated microphone. Results of this study indicate that with all tested users SkullConduct had a probability of around 97% when it comes just to identify a correct user. Test of the system as an authentication tool showed an Equal Error Rate (EER) of around 6.9% in average but with significant drops the shorter the used sample gets (less than 1 second).

Other work on authentication via smart devices includes e.g. the works from A. Johnston et al. who implemented a smartwatch based authentication module that used gait recognition [6]. They adapted from previous work of theirs where gyro- and acceleration-sensors of smart phones were used to develop authentication methods [8]. The main thought behind the proposed use of gait authentication on smartwatches is that their place of wearing/usage is more consistent than the one of a smart phone and therefore more advantageous. Each participants dataset includes both data from gyro- and acceleration-sensor. Tests in regard of both design types showed that the general performance of authentication is way higher in average than the one of identification (e.g. 97.2% compared to 79.2%). Additionally the overall performances of the acceleration-sensor was higher than the gyro-sensor. Conclusions Johnston et al. drew from their results were that it is possible to authenticate someone sufficient enough using a smartwatch but they propose not to use the system for something other than a multi-modal biometric system at its current level.

3 Concept

4 Implementation

5 Evaluation

6 Conclusion

References

1. Themenseite: Wearables, https://de.statista.com/themen/3471/wearables/
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. Johnston, A.H., Weiss, G.M.: Smartwatch-based biometric gait recognition. In: 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS). pp. 1–6. IEEE (2015)
7. 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)
8. Kwapisz, J.R., Weiss, G.M., Moore, S.A.: Cell phone-based biometric identification. In: 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS). pp. 1–7. IEEE (2010)
9. Liebers, J., Schneegass, S.: Introducing functional biometrics: Using body-reflections as a novel class of biometric authentication systems. In: Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems Extended Abstracts. pp. 1–7 (2020)
10. 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
11. 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)
12. Wayman, J., Jain, A., Maltoni, D., Maio, D.: An introduction to biometric authentication systems. In: Biometric Systems, pp. 1–20. Springer (2005)
13. Yampolskiy, R.V., Govindaraju, V.: Behavioural biometrics: a survey and classification. International Journal of Biometrics **1**(1), 81–113 (2008)
14. Yang, J., Li, Y., Xie, M.: Motionauth: Motion-based authentication for wrist worn smart devices. In: 2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops). pp. 550–555. IEEE (2015)