Bachelorprojekt
Functional Biometric Authentication using Sound on Smart Devices

Johannes Waltmann

University of Duisburg-Essen
Matriculationnumber: 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 caused by the many sensors built in these devices and their ability to capture sensible personal information (e.g. health informations). Additionally smart devices can now also 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. In the current general smart-wearable design neither of these sensors is oriented towards the wearers arm. With a change in position of these sensors smartwatches become eligible for functional biometric authentication. Further motivation for this new authentication method comes from the fact that the previous classical methods (PIN, password...) are not suited for usage on smartwatches [17]. Nevertheless it is shown by Johnston [9] and Yang [19] in their respective works that there already are potential biometric authentication methods for smartwatches based on distinct hand or arm movements.

From these preconditions a prototype is defined. This prototype uses a sound based functional biometric which gets applied to its wearers arm.

2 Related Work

This section will give an overview on the terms of biometrics and its variations, authentication and also what defines an authentication system. Additionally an insight into other works on biometric or smartwatch based authentication will be provided.

2.1 Authentication

The term in general describes the process based on which a security systems tries to approve someone's claim of identity [3]. Based on the input type of this claim the term authentication can be further subdivided into explicit and implicit authentication. *Explicit* authentication is more often also known as traditional authentication [13]. This includes providing knowledge like PIN or password, using a token but also performing gestures, fingerprints etc. from the biometrical field.

Implicit authentication on the other hand describes mechanisms where a user does not provide a password, etc. directly. Instead users are authenticated based on observations of their behavioural patterns[8]. These observations are qualified for the use in e.g. biometrics since every individual has its own distinct habits which could be captured and analysed using different sensors [15]. Furthermore Shi, Jakobsson et al. state in their 2009 and 2010 works that implicit authentication is well suited for usage in combination with mobile smart-devices [15] or portable computers [8]. Based on this they propose three different application scenarios. 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 e.g. financial actions on a mobile device.

2.2 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 of 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 geometry or the specific way someone interacts [7, chpt. 1.1][5]. Depending on the concept of usage a biometric system can be used in either verification or identification mode [7, chpt. 1.3]. These two modes can also be differed by the use of *positive* or *negative identification* techniques [16].

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 are provided the general term of biometrics can be further divided into behavioural and physiological biometrics. Also a new kind of biometrics called functional biometrics was introduced by Liebers and Schneegass in 2020 [12].

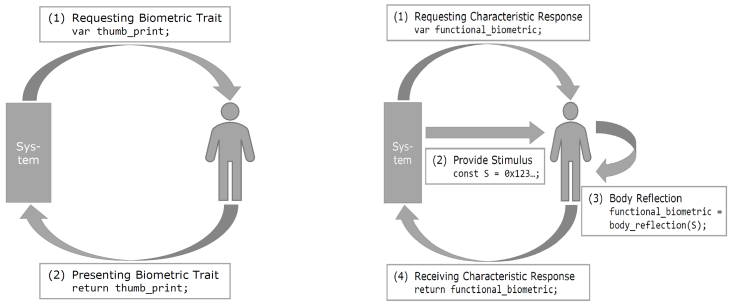
Behavioural Biometrics Behavioural biometrics refers to authentication systems in which the process of authentication is related to the behaviour of an individual [3]. In most cases this process is conducted with the use of primarily gestures or other actions or movements capable of being performed in everyday life [18]. Features which can be used for behavioural biometrics include e.g gait, keystrokes but also authentication patterns on smartphones could be used. One main advantage compared to physiological biometrics is that some behavioural

traits must not be collected actively but can be captured whilst performing any kind of different tasks [18]. Also there is no definite need for special hardware since the sensors needed are mostly built in smart wearables which are one of the main users of behavioural biometrics [9].

Physiological Biometrics Apart from behavioural biometrics the classification of physiological biometrics is also existent. This form of biometric authentication uses the more "static" traits of a users body as token such as e.g. fingerprints, hand geometry [2] or vein patterns [6].

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. [10], [5].

Functional Biometrics With functional biometrics another novel kind of biometric authentication was introduced lately by Liebers and Schneegass [12]. This new concept stands as a major influence to this work notably with its first implementation in SkullConduct[14].



(a) Traditional Biometrics (b) Functional Biometrics

Figure 1. (a) shows the authentication process of a traditional biometric system where a characteristic response is created based on someone's unique trait. (b) shows the order of steps for functional biometrics when a stimulus is added to create the characteristic based on body reflections [12].

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 (cf. 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.

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 [9]. They adapted from previous work of theirs where gyro- and acceleration-sensors of smart phones were used to develop authentication methods [11]. 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

Even though the technology of smart devices has become more popular over the last recent years it still does take some effort to protect them sufficiently in comparison to e.g. smartphones. These smart devices need personal authentication

because they can collect sensible data while in usage, could be used to display instant messages or can be used as a payment method with integrations of applications such as paypal or apple pay. Possible solutions to solve this could be traditional authentication methods even though it can be tricky executing them since smart watches normally have very little displays whereas other smart devices could not even have a display on which a pin or security pattern could be entered.

An early example of using (smart)devices as an extra medium for authentication comes form Corner and Noble in their 2002 work "Zero-Interaction Authentication"[4]. There they provided an implicit decryption system for laptops which relies on a wearable token generator to implicitly generate and send the decryption keys when they are needed. One example they proposed for the use as the token generator was an IBM Linux watch, an early 2000s predecessor from the nowadays smartwatch.

The introduction of behavioural biometrics showed alternatives to these previously describes methods. Analysing e.g. the uniqueness of an individuals movements or other behaviour these biometric mechanisms do not rely on the use of knowledge based authenticators like the traditional methods.

Another alternative to these two types of authentication would be the use of the new approach on functional biometrics. For example, a smartwatch based authentication system which uses functional biometrics could send a stimulus on an interval base whose alteration is compared to a previously stored default value. The advantage of this functional approach against the behavioural one is that, even though both are implicit, movements or behaviours could still be mimicked whereas the transformation of the functional system is based on someone's body structure e.g. the done density.

Possible stimuli could be sound patters which use either white noise, frequency changes or little melodies. The stimulus can then be applied to the wearer on a regular base over the time the device is worn to ensure it is used by the correct user. Also if the stimulus used gets leaked or corrupted otherwise a functional biometric system does not need to be recalibrated completely. Since even the system itself does not really know the nature of the transformation function only a new stimulus and new sample data are needed.

4 Implementation

5 Evaluation

6 Conclusion

References

1. Themenseite: Wearables (Mar 2020), https://de.statista.com/themen/3471/wearables/, retrieved on 07.05.2020
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. Bhattacharyya, D., Ranjan, R., Alisherov, F., Choi, M., et al.: Biometric authentication: A review. International Journal of u-and e-Service, Science and Technology **2**(3), 13–28 (2009)
4. Corner, M.D., Noble, B.D.: Zero-interaction authentication. In: Proceedings of the 8th Annual International Conference on Mobile Computing and Networking. p. 1–11. MobiCom '02, Association for Computing Machinery, New York, NY, USA (2002)
5. 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)
6. 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)
7. Jain, A.K., Flynn, P., Ross, A.A.: Handbook of biometrics. Springer Science & Business Media (2007)
8. Jakobsson, M., Shi, E., Golle, P., Chow, R.: Implicit authentication for mobile devices. In: Proceedings of the 4th USENIX conference on Hot topics in security. pp. 9–9 (2009)
9. 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)
10. 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)
11. 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)
12. 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)
13. Ranjan, J., Whitehouse, K.: Automatic authentication of smartphone touch interactions using smartwatch. In: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct. pp. 361–364 (2016)
14. 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

15. 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)
16. Wayman, J., Jain, A., Maltoni, D., Maio, D.: An introduction to biometric authentication systems. In: Biometric Systems, pp. 1–20. Springer (2005)
17. Xu, W., Shen, Y., Zhang, Y., Bergmann, N., Hu, W.: Gait-watch: A context-aware authentication system for smart watch based on gait recognition. In: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation. pp. 59–70 (2017)
18. Yampolskiy, R.V., Govindaraju, V.: Behavioural biometrics: a survey and classification. International Journal of Biometrics **1**(1), 81–113 (2008)
19. 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)