Introducing Functional Biometrics: Using Body-Reflections as a Novel Class of Biometric Authentication Systems

Jonathan Liebers
University of Duisburg-Essen
jonathan.liebers@uni-due.de

Stefan Schneegass
University of Duisburg-Essen
stefan.schneegass@uni-due.de

CHI '20 Extended Abstracts, April 25–30, 2020, Honolulu, HI, USA.

ACM ISBN 978-1-4503-6819-3/20/04.
http://dx.doi.org/10.1145/3334480.3383059

Abstract

Human-computer authentication is a continuously important topic where besides security also the aspects of usability must be taken into consideration. Biometric authentication methods promise to fulfill both aspects to a high degree, yet they come with severe drawbacks, such as the lack of changeability of the utilized trait, in case it is leaked or stolen. To compensate for these disadvantages, we introduce a novel class of biometric authentication systems in this work, named "Functional Biometrics". This approach regards the human body as a function that transforms a stimulus which is applied to the body by the authentication system. Both, the stimulus and the measured body reflection form a pair that can subsequently be used for authentication, yet the underlying function remains secret. Following this approach, we intend to disprove some of the drawbacks of traditional biometrics.

Author Keywords

Authentication; Functional Biometrics; Usable Security.

CCS Concepts

•**Security and privacy** → *Usability in security and privacy;*
•**Human-centered computing** → *Human computer interaction (HCI);*

Attack Vectors

Similar to other types of authentication, biometric authentication is prone to certain attack vectors. With advancement in fabrication tools (e. g., 3D printers), the possibility to create physical tokens that can be used to grant unauthorized access to systems secured with biometrics is constantly increasing [6].

Similarly, face recognition systems have been tricked with simple print outs of a face that made liveness detection a necessity [10].

To mitigate the threat of stolen biometric traits, anti-spoofing measures were introduced [12], as well as multi-modal biometrics [14] and cancellable biometrics [13] that apply a non-revertible transform to the recorded biometric trait before it is stored by the system.

Introduction

The number of systems requiring user authentication is increasing every year. In 2019, the company "LastPass" which offers a password manager for over 17.8 million users stated that an employee of a small business needs to remember in average 85 passwords [4]. Traditional approaches to authentication such as personal identification numbers and passwords overwhelm users since they have to remember dozens of them and research has also shown that the selection of user-generated passwords is predictable [3, 15, 20]. Passwords are furthermore prone to theft and tend to be reused [20]. To counteract these weaknesses, devices such as smartphones and laptops are often equipped with biometric authentication mechanisms [5].

While biometrics nowadays provide sufficient security for most application scenarios, in the aspects of usability, they are rated higher by the user than knowledge-based authentication methods [1]. Yet, biometric methods are also affected by severe drawbacks. First, a person is in general unable to change their physiological biometric trait, in case it is leaked by the underlying system. Second, many biometric traits are involuntarily shared with the surrounding environment on a regular basis. For example, the required fingerprints for fingerprint recognition can easily be acquired as they are left on every object that is touched by the user. For facial recognition, the required photography of the user can often easily be acquired or can sometimes simply be collected from the internet.

Our goal is to create more secure authentication systems that are convenient for the user to use and overcome the shortcomings of the current biometric methods. We establish a novel class of biometrics that is based on body-reflections. In our vision, the body of a person is utilized as a function. A stimulus is applied to the body of the user and a measurement is made, how the body transforms the applied stimulus.

Biometric Authentication

To authenticate against a computing system which utilizes biometric authentication, the user needs to present a characteristic biometric trait of him or her to the system. This trait can be a physiological (e. g., fingerprint, face geometry, vein pattern [7]) or behavioral attribute (e. g., the specific way of interacting with an input device) of a person [8].

In terms of usability, biometric authentication systems can be distinguished into systems implementing "explicit" and "implicit" authentication. The notion is similar to implicit and explicit interactions [16]. Explicit authentication means, that a user needs to explicitly interact with the authentication system, e. g., by providing a password upon facing a password prompt throughout using a website. Implicit authentication on the other hand is defined as the ability to authenticate users based on actions "they would carry out anyway" [9]. As a consequence, implicit authentication can be transparent to the user.

To evaluate the performance of biometric authentication systems, many different approaches and metrics are used across researchers. As the evaluation methods and reported performance metrics differ, the results are often only hardly comparable. To consolidate the metrics used for the evaluation of biometric authentication systems, Sugrim et al. proposed to report the unnormalized frequency count of scores in combination with the receiver operating characteristics curve [19]. Reporting these two metrics attributes to the comparability of research.

Biometric authentication systems are moreover prone to certain attack vectors, resulting in a spoofing of identity. The sidebar provides further insights on this subject.

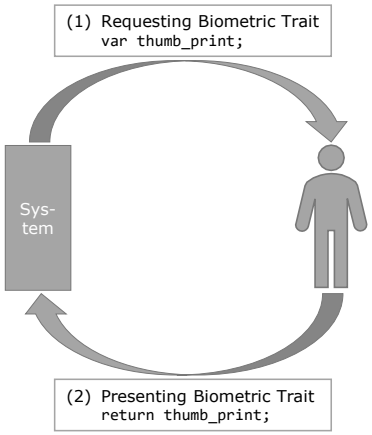

Figure 1: Traditional biometric authentication systems request and verify a physiological or behavioral trait of a person. The physiological trait behaves similar to a token, as the user presents it to the authentication system's sensors.

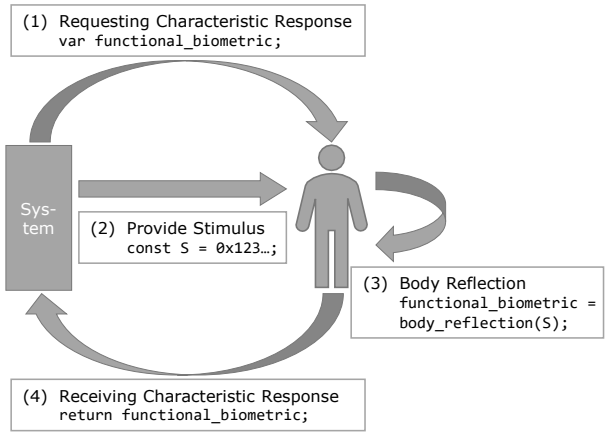

Figure 2: Functional Biometric systems authenticate based upon a characteristic response that the user generates through body reflection. The SGU applies a stimulus in step (2) that is transformed through body reflection in step (3). The BRS captures the transformed value in step (4).

Functional Biometrics

We introduce "Functional Biometrics" as a novel class of biometrics (cf., Figure 2). In contrast to biometric systems that are based on physiological or behavioral characteristics (cf., Figure 1), this class exploits the user's body as a function. This class of biometrics does not only rely on a trait that is handled like a token. Instead, a signal stimulus is generated and applied to the human body by the system the user authenticates against. Thus, it combines the properties of both classical types of biometrics.

This signal is modified by the user's body which in return generates a characteristic response through the user's unique body reflection. This characteristic response then forms a single point of a user's body reflection function for the given stimulus. It is measured by the system and compared to a pre-stored response to authenticate the user.

Each system utilizing Functional Biometrics needs to be composed of at least two specialized hardware components. First, a Stimulus Generation Unit (SGU) is required, which generates a signal and applies it to the user's body. The SGU either generates a constant stimulus or varies it over a period of time in a specific pattern. The type of the applied stimulus can be of many kinds. We envision audio and haptic stimuli, as well as electrical signals (i. e., such as in electrical muscle stimulation). Second, a Body Reflection Sensor (BRS) is required that records the propagated body reflection and which must be designed as a dependency of the SGU. The BRS captures the response of the body, i. e.,

the result of the body's reflection function applied to the stimulus. The type of the captured response can range from propagated audio, over movement patterns to specific muscle reactions. Additionally, the components of a traditional biometric authentication system are required, which might include a quality assessment and feature extraction module, a matching and decision-making module and a system database module [8] or further machine learning methods. Those components process the input-pattern of the stimulus that the SGU generates and the output-pattern of the body reflection which the BRS captures to form a point, akin to a challenge-response-authentication system.

The body reflection function is an individual, private attribute of a person that remains secret at all time. The authentication system generates a pair $(x, f(x))$ which is a point of the body reflection function f, where x is the stimulus applied by the SGU and $f(x)$ is the transformation that is captured by the BRS. This pair is the secret that is stored by the authentication system and utilized in the process of authentication by re-applying the x with the SGU and expecting the associated $f(x)$ throughout the BRS. If, in any case, the software system leaks or loses this information, a new pair can be generated and stored, discarding the old pair. As the stimulus which is generated by the SGU can be varied over an indeterminate period of time, a space enfolds that can contain a multitude of points for a user's body reflection function.

Exemplary Authentication Systems
An example of the presented principle of Functional Biometrics is "SkullConduct" [18] that utilizes the bone conduction of sound through the user's skull (cf., Figure 3). Moreover, we are working on a prototype to demonstrate the effect of heat transfer on the contrast of a user's vein pattern that is captured by a thermal imager. We intend to place the SGU

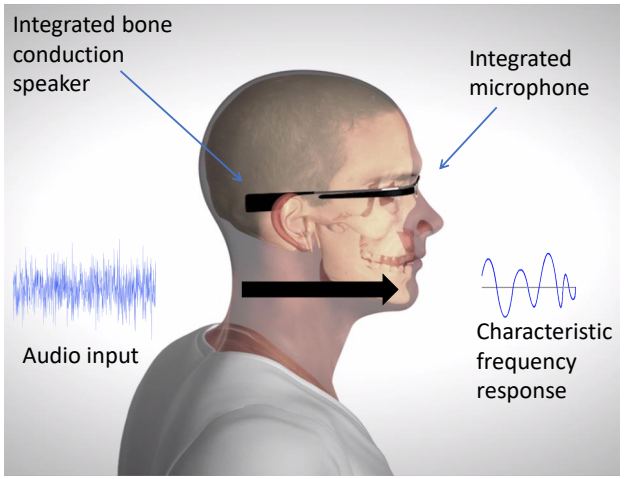

Figure 3: "SkullConduct" is the first authentication system that successfully utilizes Functional Biometrics [18] on smart glasses.

at the wrist of the user, letting it emit an adequate amount of heat, which then is transferred to the back of the hand. The heat should influence the vein pattern's contrast over time. A thermal imager is the BRS that captures a thermal image of the back of the hand, where a change in contrast over time should become apparent. The speed and intensity of the heat transfer are defined by the body reflection function. We also envision to utilize the impact of haptic feedback on the user (e. g., by picking up a vibrating smartphone). The vibration motor shakes the smartphone in a specific pattern, emitting a haptic force as the SGU. The user then picks the phone up and the arm should be moved at an individual intensity, reducing the shaking of the phone. As the BRS, the gyrosensor of the phone could measure the motion and shaking intensity of the arm, that is determined by the individual body reflection function.

Discussion

Functional Biometrics combines the advantages of common knowledge-based authentication approaches such as alphanumeric passwords (i. e., they are changeable and a multitude of passwords per user might exist) with the advantages of biometric authentication approaches such as fingerprints (i. e., no cognitive load and no memorability required). Different systems can use different stimuli and, thus, a compromised system does not result in every system being compromised.

We expect that this approach is particularly useful for wearable devices such as smartwatches or smart glasses. While these devices traditionally lack proper authentication methods due to the absence of appropriate input methods [2, 11, 17], authentication systems using functional biometrics can exploit the close proximity to the body for inducing a signal and measuring the characteristic response. We furthermore regard this approach to be in particular very convenient to the user, as authentication systems, implementing Functional Biometrics should be inherently capable of implementing implicit authentication. This could also eliminate the need of bothering the user with authentication requests during his or her interaction with a device.

We believe that this approach realizes unique benefits, such as the acquisition of an indefinite amount of points for a person's body reflection function. Subsequently, a leak of information or the theft of a biometric trait is not a concern anymore, since another characteristic response can be acquired for a different stimulus. As the body reflection function can only be approximated point-by-point by applying a stimulus to a person, the underlying function remains secret and private at all times. Moreover, the acquisition of such a point is not or only hardly achieved undetected, as the user would likely notice when a stimulus is applied from an external, unexpected source.

Summary

In this work we establish "Functional Biometrics" as a novel class of biometric authentication systems. In contrast to traditional biometric authentication systems that utilize a physiological or behavioral trait, Functional Biometrics utilize the user's body as a function. This function transforms a stimulus, that is applied to the user's body and is subsequently captured. The function acts as the user's biometric secret, that cannot be lost, stolen or leaked. Additionally, a multitude of points can be generated from the body reflection function, so that the loss or leak of one point is not a fundamental problem anymore since it can easily be replaced. We furthermore envision this approach to be in particular useful for body-near devices such as smartwatches or smart glasses, being able to implement an implicit authentication scenario. A first implementation of the presented principle already exists in the form of "SkullConduct" [18].

Acknowledgement

The presented work was funded by the German Research Foundation (DFG) under project no. 426052422.

REFERENCES

[1] Rasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides. 2015. Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption. (2015). https://doi.org/10.14722/usec.2015.23003

[2] Andrea Bianchi and Ian Oakley. 2016. Wearable authentication: Trends and opportunities. *it-Information Technology* 58, 5 (2016), 255–262.

[3] J. Bonneau. 2012. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In *2012 IEEE Symposium on Security and Privacy*. 538–552. DOI: http://dx.doi.org/10.1109/SP.2012.49

[4] LastPass by LogMeIn. 2019. The 3rd Annual Global Password Security Report. (2019). https://www.lastpass.com/business/articles/password-benchmark-report/thank-you

[5] Ivan Cherapau, Ildar Muslukhov, Nalin Asanka, and Konstantin Beznosov. 2015. On the Impact of Touch ID on IPhone Passcodes. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security (SOUPS '15)*. USENIX Association, USA, 257–276.

[6] J. J. Engelsma, S. S. Arora, A. K. Jain, and N. G. Paulter. 2018. Universal 3D Wearable Fingerprint Targets: Advancing Fingerprint Reader Evaluations. *IEEE Transactions on Information Forensics and Security* 13, 6 (June 2018), 1564–1578. DOI: http://dx.doi.org/10.1109/TIFS.2018.2797000

[7] Sarah Faltaous, Jonathan Liebers, Yomna Abdelrahman, Florian Alt, and Stefan Schneegass. 2019. VPID: Towards Vein Pattern Identification Using Thermal Imaging. *i-com* 18, 3 (2019), 259–270. https://dx.doi.org/10.1515/icom-2019-0009

[8] Anil K. Jain, Patrick Flynn, and Arun A. Ross. 2007. *Handbook of Biometrics*. Springer-Verlag, Berlin, Heidelberg. https://dx.doi.org/10.1007/978-0-387-71041-9

[9] Markus Jakobsson, Elaine Shi, Philippe Golle, and Richard Chow. 2009. Implicit authentication for mobile devices. In *Proceedings of the 4th USENIX conference on Hot topics in security*. 9–9.

[10] K. Kollreider, H. Fronthaler, and J. Bigun. 2009. Non-Intrusive Liveness Detection by Face Images. *Image Vision Comput.* 27, 3 (Feb. 2009), 233–244. DOI: http://dx.doi.org/10.1016/j.imavis.2007.05.004

[11] A. Lewis, Y. Li, and M. Xie. 2016. Real time motion-based authentication for smartwatch. In *2016 IEEE Conference on Communications and Network Security (CNS)*. 380–381. DOI: http://dx.doi.org/10.1109/CNS.2016.7860521

[12] Sébastien Marcel, Mark S. Nixon, Julian Fiérrez, and Nicholas W. D. Evans (Eds.). 2019. *Handbook of Biometric Anti-Spoofing - Presentation Attack Detection, Second Edition*. Springer. DOI: http://dx.doi.org/10.1007/978-3-319-92627-8

[13] N. K. Ratha, J. H. Connell, and R. M. Bolle. 2001. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal* 40, 3 (2001), 614–634. DOI: http://dx.doi.org/10.1147/sj.403.0614

[14] A. Ross and A. K. Jain. 2004. Multimodal biometrics: An overview. In *2004 12th European Signal Processing Conference*. 1221–1224.

[15] Florian Schaub, Ruben Deyhle, and Michael Weber. 2012. Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia (MUM '12)*. Association for Computing Machinery, New York, NY, USA, Article Article 13, 10 pages. DOI: http://dx.doi.org/10.1145/2406367.2406384

[16] Albrecht Schmidt. 2000. Implicit human computer interaction through context. *Personal Technologies* 4, 2 (01 Jun 2000), 191–199. DOI: http://dx.doi.org/10.1007/BF01324126

[17] Stefan Schneegass, Thomas Olsson, Sven Mayer, and Kristof van Laerhoven. 2016a. Mobile Interactions Augmented by Wearable Computing: A Design Space and Vision. *Int. J. Mob. Hum. Comput. Interact.* 8, 4 (Oct. 2016), 104–114. DOI: http://dx.doi.org/10.4018/IJMHCI.2016100106

[18] Stefan Schneegass, Youssef Oualil, and Andreas Bulling. 2016b. 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 (CHI '16)*. Association for Computing Machinery, New York, NY, USA, 1379–1384. DOI: http://dx.doi.org/10.1145/2858036.2858152

[19] Shridatt Sugrim, Can Liu, Meghan McLean, and Janne Lindqvist. 2019. Robust Performance Metrics for Authentication Systems. In *NDSS*. https://www.ndss-symposium.org/ndss-paper/robust-performance-metrics-for-authentication-systems/

[20] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. 2016. Understanding Password Choices: How Frequently Entered Passwords Are Re-used across Websites. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 175–188. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/wash