Single-Sign-On in Smart Homes using Continuous Authentication

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

Nick Wittig
nick.wittig@uni-due.de
University of Duisburg-Essen
Essen, Germany

Simon Janzon
simon.janzon@uni-due.de
University of Duisburg-Essen
Essen, Germany

Pedram Golkar
pedram.golkar@stud.uni-due.de
University of Duisburg-Essen
Essen, Germany

Hakeem Moruf
hakeem.moruf@stud.uni-due.de
University of Duisburg-Essen
Essen, Germany

Wilfried Wakeu Kontchipo
wilfried.wakeu-kontchipo@stud.uni-due.de
University of Duisburg-Essen
Essen, Germany

Uwe Gruenefeld
uwe.gruenefeld@uni-due.de
University of Duisburg-Essen
Essen, Germany

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

ABSTRACT

Modern ubiquitous computing environments are increasingly populated with smart devices that need to know the identity of users interacting with them. At the same time, the number of authentications that a user needs to perform increases, as nowadays devices such as smart TVs require authentication which was not the case in earlier times. Even for single-person households, the need to authenticate against present smart devices in the environment appears at regular intervals, ranging from TVs to voice assistants, to gaming consoles. To reduce the need for repeated authentication, we explore the concept of a system that allows the sharing of users' authenticated identity information between smart devices, similar to the concept of Single-Sign-On on the internet. Following a preliminary field study, we show that such a system can decrease the number of necessary authentications in a ubiquitous computing environment by 84.4%, increasing usability and security.

CCS CONCEPTS

• **Security and privacy** → *Usability in security and privacy.*

KEYWORDS

continuous user authentication, usable security, single sign on

ACM Reference Format:

Jonathan Liebers, Nick Wittig, Simon Janzon, Pedram Golkar, Hakeem Moruf, Wilfried Wakeu Kontchipo, Uwe Gruenefeld, and Stefan Schneegass. 2022. Single-Sign-On in Smart Homes using Continuous Authentication. In *21th International Conference on Mobile and Ubiquitous Multimedia (MUM 2022), November 27–30, 2022, Lisbon, Portugal.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3568444.3570595

MUM 2022, November 27–30, 2022, Lisbon, Portugal

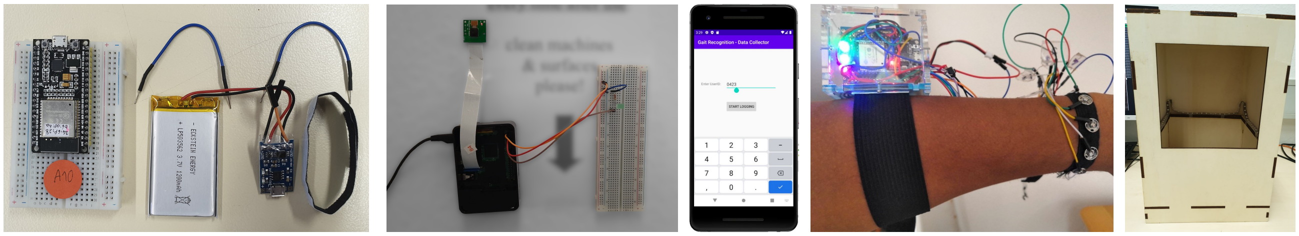
ACM ISBN 978-1-4503-9820-6/22/11.
https://doi.org/10.1145/3568444.3570595

1 INTRODUCTION

The number of systems requiring user authentication is increasing yearly, and each person possesses a growing amount of online accounts [3]. This trend also takes place in the domain of ubiquitous computing environments [22] such as smart homes, as the number of installed smart devices increases over time [15]. Currently, a typical household is populated with devices that are often shareable between the inhabitants such as desktop computers, smart TVs, smart locks, or virtual reality headsets, which all need to know the user's identity [8]. They have in common that their means for authentication are isolated and that the determined identity is not shareable with other devices. However, their authentication usability is vastly different as using face-id is easier than entering a password on a smart TV [10]. To relieve users of frequently re-authenticating themselves in their homes, we envision a system that enables the sharing of a person's identity information between devices after authentication. Hence, we present a single-sign-on (SSO) system [14] for smart homes that reduces the number of necessary authentications by over 80%, making use of an indoor localization system. We extend on the work done by Bardram [1], who encountered the same challenges in a ubiquitous computing environment of a clinic, by moving a step further by creating an implementation that is evaluated in a preliminary field study.

2 CONCEPT & IMPLEMENTATION

To reduce the number of interactions with authentication systems, we design a continuous authentication system that can share the identity information of an authenticated user between several connected smart devices [20]. To do so, our system localizes the smart home's inhabitants [19] and makes predictions about their activities [21]. Once a user authenticates successfully against one of the connected devices, the system retrieves this identity information and automatically unlocks other devices, when the user moves into their proximity. The design consists of three components: i) an Authentication Brokerage Service (ABS), ii) a Localization System (LS), and iii) a flexible variety of four different User Authentication Devices (UAD), recreated from previous work.



(a) Localization System Anchor. (b) Face Recognition Module. (c) Gait App. (d) Bioimpedance System. (e) Hand Geometry.

Figure 1: Photographies of the localization system in (a) and the four user authentication devices in (b) to (e).

2.1 Authentication Brokerage Service (ABS) and Localization System (LS)

The ABS is the central hub of information within the ubiquitous computing environment, connected to the Localization System, the User Authentication Devices, and all other devices. It obtains the user's current authentication status and their positional information, knowing which user authenticated against which device at what point in time. The ABS is in charge of locking and unlocking devices and takes care of authorization levels and conflicts and unlocks devices if only a single authorized user is near the device. For the LS, we created 14 ESP32 micro-controllers (cf., Figure 1(a)) placed in our office environment (cf., Figure 2), acting as anchors to receive the users' smartphones Bluetooth RSSI [16], reporting this information to the ABS via WiFi. The LS is a critical security component, as it must not be tampered with, i. e., the user must not be able to influence the localization system maliciously. Following a short evaluation, we find a mean positional error of 1.5 - 2 m for the LS.

2.2 User Authentication Devices (UAD)

We recreate four different user authentication devices (UAD) from previous works [4–7, 12, 17, 18]. The implementations are shown in Figure 1.

2.2.1 UAD Nr. 1: Face Recognition. The face recognition prototype is created of a Raspberry Pi 3 with a Pi Camera Module (cf., Figure 1(b)), performing face detection and -recognition. We implemented face detection using pre-trained Haar features to detect faces with OpenCV [2, 13]. After a face is detected, its identity is verified using a Local Binary Pattern Histogram (LBPH). We evaluate this module's performance on an altered version of the AT&T Database of Faces [17] with an addition of 10 images of faces that are not classified with labels to be rejected (in total 370 faces of labeled persons and 10 faces of non-labeled persons), reaching an accuracy of 97.87%. As face recognition captures the users' faces while they perform another activity, it is capable of implicit authentication.

2.2.2 UAD Nr. 2: Gait Recognition. The gait recognition system is a mobile and implicit authentication system for Android (cf., Figure 1(c)), following the work of Derawi et al. [6] and Muaaz et al. [12]. We use the phone's accelerometer to collect movement data at 50 Hz and apply a walking detection by applying a sliding window and a variance detection, combining a cycle length estimation and -detection. Unusual cycles are removed using DTW [11]. In a pre-study, we find an accuracy of 83.88% for authentication across two days ($N = 5$).

2.2.3 UAD Nr. 3: Bio-Impedance Recognition. The bio-impedance recognition module is a mobile and implicit functional biometric authentication system that alternates current resistance between two electrodes attached to the body through a wristband based on the work of Cornelius et al. [4, 5, 9]. Providing a stimulus in the form of a low voltage, it measures impedance in the body formed by features such as bone shape and tissue. We combine an ESP32 with an AD5933 chip that performs frequency sweeps (cf., Figure 1(d)) and find in a pre-study ($N = 7$) an accuracy of 95.56% [4, 5].

2.2.4 UAD Nr. 4: Hand Geometry Recognition. We moreover implemented an explicit hand geometry recognition system that identifies people by the geometric features of their hands (e. g., their width and length of fingers) that are captured through a Raspberry Pi 3 and a Raspberry Pi Camera module within a plywood box (cf., Figure 1(e)). It recognizes the hand geometry and palm print texture of a hand in the box, combining the work of Sharma et al. and Jaswal et al. [7, 18]. A pre-study ($N = 15$) with three samples per participant showed an authentication accuracy of 83%.

3 RESULTS OF A PRELIMINARY FIELD STUDY

We conducted a preliminary field study in the regular office environment of our institute (cf., Figure 2) to evaluate our system for a duration of 118 minutes. In total, five persons working there participated in the study together with two visitors. The five present participants were registered with the system, i. e., their identity was known to the ABS and they were authorized to use any device, and two visitors were marked as unauthorized guests to be rejected by any device. All participants were provided a smartphone that acts as a beacon for the localization system.

Following our field study, we focus on saving the users' authentication attempts compared to systems that require individual authentication for each device. In total, there were 33 authentications during the field study, including 22 authentications from study participants whose biometric data was stored in the database of the ABS. All in all, 141 activations of smart devices (cf., Figure 2) were logged during the study. Thus, assuming that conventional systems require one authentication for each unlock, our system achieves a saving of 119 authentications, resulting in a reduction of 84.4% compared to conventional authentication systems, where each device authenticates users on its own.

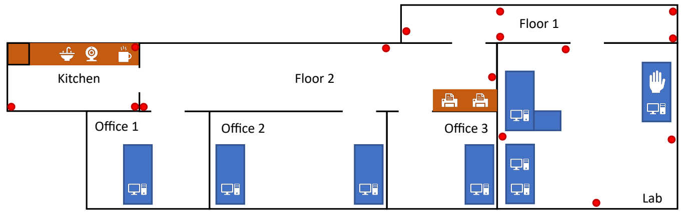


Figure 2: Map of our office environment (not to scale). Blue areas mark office desks and brown areas general purpose desks (e.g., countertop in the kitchen). Red dots symbolize the deployed ESP32 localization anchors. Offices were exempt from the field study. The webcam icon symbolizes the face recognition module and the hand icon the hand geometry recognition module. Gait recognition was installed on participants' smartphones used for localization. Objects that were assumed to need a person's authentication information were the coffee machine in the kitchen, the printers on floor 2, and all four computers in the lab.

4 DISCUSSION & CONCLUSION

From the obtained results, we find a reduction of 84.4% in authentication attempts that could be skipped under the assumption that the localization system found only one person being near said device. This number, however, stands on the assumption that the localization system has access to everybody's location in an environment. Our proposed concept allows the sharing of identity information between several smart devices and thus reduces the number of repeated authentications. To fulfill this goal, we combined an indoor localization technique with an authentication brokerage service that transfers identity information between devices. We acknowledge the limitations given by the duration of our pre-study and the study taking place in an office environment. In conclusion, the system reduces users' effort of authentication in smart environments.

ACKNOWLEDGMENTS

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

REFERENCES

[1] Jakob E. Bardram. 2005. The trouble with login: on usability and computer security in ubiquitous computing. *Personal Technologies* 9, 6 (2005), 357–367. https://doi.org/10.1007/s00779-005-0347-6

[2] G. Bradski. 2000. The OpenCV Library. *Dr. Dobb's Journal: Software Tools for the Professional Programmer* 25, 11 (2000), 120–123.

[3] LastPass by LogMeIn. 2019. *The 3rd Annual Global Password Security Report.* https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/LMI0828a-IAM-LastPass-State-of-the-Password-Report.pdf

[4] Cory Cornelius, Ronald Peterson, Joseph Skinner, Ryan Halter, and David Kotz. 2014. A wearable system that knows who wears it. In *Proceedings of the 12th annual international conference on Mobile systems, applications, and services (ACM Digital Library)*, Andrew Campbell (Ed.). ACM, New York, NY, 55–67. https://doi.org/10.1145/2594368.2594369

[5] Cory Cornelius, Jacob Sorber, Ronald Peterson, Joe Skinner, Ryan Halter, and David Kotz. 2012. Who Wears Me? Bioimpedance as a Passive Biometric. In *3rd USENIX Workshop on Health Security and Privacy (HealthSec 12)*. USENIX Association, Bellevue, WA. https://www.usenix.org/conference/healthsec12/workshop-program/presentation/Cornelius

[6] Mohammad Omar Derawi, Claudia Nickel, Patrick Bours, and Christoph Busch. 2010. Unobtrusive User-Authentication on Mobile Phones Using Biometric Gait Recognition. In *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, 306–311. https://doi.org/10.1109/IIHMSP.2010.83

[7] Gaurav Jaswal, Amit Kaul, and Ravinder Nath. 2019. Multimodal Biometric Authentication System Using Hand Shape, Palm Print, and Hand Geometry. In *Computational Intelligence*, Nishchal K. Verma (Ed.). Advances in Intelligent Systems and Computing Ser, Vol. 799. Springer, Singapore, 557–570. https://doi.org/10.1007/978-981-13-1135-2_42

[8] Jonathan Liebers, Mark Abdelaziz, Lukas Mecke, Alia Saad, Jonas Auda, Uwe Gruenefeld, Florian Alt, and Stefan Schneegass. 2021. Understanding User Identification in Virtual Reality Through Behavioral Biometrics and the Effect of Body Normalization. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411764.3445528

[9] Jonathan Liebers and Stefan Schneegass. 2020. 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 (CHI EA '20)*. Association for Computing Machinery, New York, NY, USA, 1–7. https://doi.org/10.1145/3334480.3383059

[10] Lukas Mecke, Ken Pfeuffer, Sarah Prange, and Florian Alt. 2018. Open Sesame! User Perception of Physical, Biometric, and Behavioural Authentication Concepts to Open Doors. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia* (Cairo, Egypt) *(MUM 2018)*. Association for Computing Machinery, New York, NY, USA, 153–159. https://doi.org/10.1145/3282894.3282923

[11] Meinard Müller. 2007. Dynamic Time Warping. In *Information Retrieval for Music and Motion*, Meinard Müller (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 69–84. https://doi.org/10.1007/978-3-540-74048-3_4

[12] Muhammad Muaaz and René Mayrhofer. 2016. Accelerometer based Gait Recognition using Adapted Gaussian Mixture Models. In *Proceedings of the 14th International Conference on Advances in Mobile Computing and Multi Media*. ACM, New York, NY, USA, 288–291. https://doi.org/10.1145/3007120.3007164

[13] C. P. Papageorgiou, M. Oren, and T. Poggio. 1998. A general framework for object detection. In *Proceedings / Sixth International Conference on Computer Vision*. Narosa, New Delhi, 555–562. https://doi.org/10.1109/ICCV.1998.710772

[14] Andreas Pashalidis and Chris J. Mitchell. 2003. A Taxonomy of Single Sign-On Systems. In *Information Security and Privacy*, Rei Safavi-Naini and Jennifer Seberry (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 249–264.

[15] Zion Market Research. 2018. Global Smart Home Market to Exceed $ 53.45 Billion by 2022. https://www.globenewswire.com/news-release/2018/01/03/1281338/0/en/Global-Smart-Home-Market-to-Exceed-53-45-Billion-by-2022-Zion-Market-Research.html

[16] Mohamed Er Rida, Fuqiang Liu, Yassine Jadi, Amgad Ali Abdullah Algawhari, and Ahmed Askourih. 2015. Indoor Location Position Based on Bluetooth Signal Strength. In *2015 2nd International Conference on Information Science and Control Engineering (ICISCE 2015)*, Shaozi Li (Ed.). IEEE, Piscataway, NJ, 769–773. https://doi.org/10.1109/ICISCE.2015.177

[17] F. S. Samaria and A. C. Harter. 1994. Parameterisation of a stochastic model for human face identification. In *Proceedings of the Second IEEE Workshop on Applications of Computer Vision*, Mary E. Kavanaugh (Ed.). IEEE Computer Society Press, Los Alamitos, Calif., 138–142. https://doi.org/10.1109/ACV.1994.341300

[18] Shefali Sharma, Shiv Ram Dubey, Satish Kumar Singh, Rajiv Saxena, and Rajat Kumar Singh. 2015. Identity verification using shape and geometry of human hands. *Expert Systems with Applications* 42, 2 (2015), 821–832. https://doi.org/10.1016/j.eswa.2014.08.052

[19] Mitilineos A. Stelios, Argyreas D. Nick, Makri T. Effie, Kyriazanos M. Dimitris, and Stelios C. A. Thomopoulos. 2008. An Indoor Localization Platform for Ambient Assisted Living Using UWB. In *Proceedings of the 6th International Conference on Advances in Mobile Computing and Multimedia* (Linz, Austria) *(MoMM '08)*. Association for Computing Machinery, New York, NY, USA, 178–182. https://doi.org/10.1145/1497185.1497223

[20] Issa Traoré and Ahmed Awad E. Ahmed. 2012. Introduction to Continuous Authentication. In *Continuous Authentication Using Biometrics: Data, Models, and Metrics*, Issa Traore and Ahmed Awad E. Ahmed (Eds.). IGI Global, Hershey, PA, USA, 1–22. https://doi.org/10.4018/978-1-61350-129-0.ch001

[21] Liang Wang, Tao Gu, Xianping Tao, Hanhua Chen, and Jian Lu. 2011. Multi-user activity recognition in a smart home. In *Activity Recognition in Pervasive Intelligent Environments*. Springer, 59–81.

[22] Mark Weiser. 1991. The Computer for the 21st Century. *Scientific American* 265, 3 (1991), 99–104.