


Privacy Aura for Transparent Authentication on Multiple Smart Devices

Takoua Guiga^{1,2}, Jean-Jacques Schwartzmann^{1,2} and Christophe Rosenberger² ^a

¹Orange Labs, France

²Normandie Univ., UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France

Keywords: Transparent Authentication, Aura, Privacy, Multi-devices.

Abstract: Nowadays, users carry multiple connected devices such as a smartphone, laptop, connected watch. . . Security constraints limit user's usability especially when using all of them intensively during the day (social media, work). In this paper, we propose the privacy Aura concept corresponding to the circle of trust in the neighborhood of each smart device to facilitate user authentication. Many data (phone calls habits, biometrics, localization) can be collected to realize a transparent and privacy compliant authentication on each device. The confidence on user authentication on each device can be transferred to another one if it is located in the same Aura. This is the main contribution of the paper. We show through illustrations the benefit of the proposed solution.


1 INTRODUCTION

Research on innovative solutions for user authentication is very active. However, while people are daily surrounded by different and multiple devices, they are still using one single device to access or protect their electronic equipment. Despite the significant rise of connected objects and Internet of Things (IoT), few are interested in the user experience taken in the totality of his/her digital interactions. If a device is compromised by attackers, security is no longer guaranteed and attackers can easily gain access to user personal data. Moreover, the authentication task requires repetitive interventions by the user as he/she has to act with different devices in its neighborhood in order to prove his/her identity to each one. With the multiplicity of authentication factors and the diversity of owned terminals, this action becomes painful and disruptive, creates stress, wastes time and clutters our daily lives with unnecessary tasks. With the intention of getting rid of the superfluous in everyday life and to ensure better security and privacy, we want to consider the multiple devices of the user in the authentication process and to delegate the authentication task to all of them. So, in case of compromise, all the devices create together a strong circle of trust, so that even when a device is stolen, it should be able to protect user's personal data. Subsequently, this

multi-devices circle is called Authentication Aura. This concept is not new as it has been proposed in (Hocking et al., 2011), we propose in this paper to extend some notions especially with a great focus on privacy. In this respect, in a ubiquitous digital environment, we propose to provide a privacy transparent authentication to the user throughout his/her day while ensuring a good privacy protection. The paper is organized as follows. Section 2 is dedicated to the related works in the area on user authentication on multiple devices. In section 3, we detail the proposed method, describing the concept, the process service and the privacy protection aspect. Section 4 provides some illustrations showing the benefit of the proposed approach. We conclude in section 5 and give some perspectives of this work.

2 RELATED WORKS

Over the recent years, it has been proven that Internet of Things (IoT) has the potential to make a society-wide impact by changing diverse sectors but also our daily lives. Despite the impressive growth of IoT-connected devices number, as mentioned in the latest Juniper Research (Juniper, 2020) claiming that the number of IoT-connected devices will reach 83 billion by 2024, rising from 35 billion connections in 2020, few research works are focusing on involving multi-devices authentication

^a  <https://orcid.org/0000-0002-2042-9029>

solutions. Multi-devices authentication, particularly the authentication Aura concept was firstly introduced by Hocking et al. (Hocking et al., 2011) as a new approach to identity authentication on mobile devices based upon a framework that can transparently improve user security confidence. Information pertaining to user authentication is shared amongst the user's devices, collectively enabling a near field adaptive security envelope to be established and maintained around the user. We can note that privacy protection was not considered in this work which is an important drawback once the General Data Protection Regulation (GDPR) is in place now for European citizens. Riva et al. (Riva et al., 2012) presented progressive authentication based on associating multiple sources of authentication data. A two-device authentication model is proposed by Cha et al. (Cha et al., 2015) for micro-payment systems using a mobile and wearable devices. Xu (Xu, 2015) focuses on biometric authentication using wearable, namely on face recognition using smart-glass and gait recognition using a smart watch. Furthermore, in order to control and secure the access to the storage services based on the cloud, Gonzalez et al. (Gonzalez-Manzano et al., 2015) propose a multi-devices solution with a symmetric cryptographic scheme. Hajny et al. (Hajny et al., 2016) presented also a cryptographic scheme providing a multi-devices authentication using wearable and IoT. Move2auth, a proximity-based mechanism for IoT device authentication was introduced by Zhang et al. (Zhang et al., 2017) based on performing hand gestures (moving towards and away, and rotating) to detect proximity and authenticate IoT devices. Nevertheless, shown results are limited on a single device which is the smartphone and there is no further analysis on other IoT devices. All these approaches lack more details about data privacy protection. On the basis of this brief overview of the literature, we can therefore agree that multi-devices authentication solutions are both limited in number and in consideration of privacy protection. Existing solutions do not focus at the same time on usability, security and privacy. In the next section, we propose a new solution extending the Aura concept by (Hocking et al., 2011). The proposed solution defines a new trust party service to Internet users respecting GDPR requirements with a great focus on usability. We describe the concept and all the steps of its usage in the following section.

3 PROPOSED METHOD

Authentication is definitely an essential and important task to secure access to our devices. At the same time, it is repetitive and painful for the user and in some cases vulnerable to attacks. Our goal in this work is to make the authentication task as simple as possible for the user while respecting his/her privacy and data security. In this section, we first introduce the concept of the authentication Aura we use in this work.

3.1 Concept Description

Surrounded by digital technology, human beings are actively interacting with digital devices during their daily life. We call this interaction digital aura translating the communication between the user and his/her digital devices through a mutual authentication. In a typical authentication scenario, the user has to realize an explicit action each time he/she wants to authenticate to all owned devices, by presenting a different code for each device, which makes ten or even twenty codes to be learned and typed hundred times a day, in order to authorize access. Our approach aims to create a multi-devices authentication system based on mutual communication between devices thanks to a trust party service (see Figure 1). We assume in this work that each device realizes a transparent authentication of the user. The idea is to define a confidence architecture between the different smart objects of the user, capable of continuously collecting behavioural or morphological data. This data must enable continuous authentication of the user. In other words, we wish to ensure sufficient interactions between a user and its devices to guarantee a high level of trust that could be transferred between them. Let's consider the following definitions:

- A : the authentication Aura of user U ,
- O_i : a device $\in A$, with $i \in [1, n_d]$, n_d is the number of devices of the user U ,
- $C(O_i)$: Confidence in a device O_i . It is computed at any time with a transparent authentication solution based on many factors (passwords, biometrics, geolocation...).

We consider that each device has its own Aura, that we call Aura device AO_i . Two types of information are sent to the trust party service: some data are transmitted to compute the confidence level associated to a device (transparent authentication scheme) and geolocation information are also transmitted in order to update the confidence level of a device O_i if it is in the Aura of a device O_j

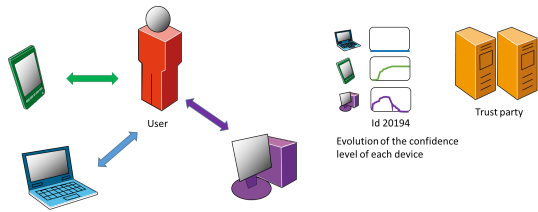


Figure 1: Principle of the proposed method: A trust party realizes the monitoring of the confidence level of each device at any time.

($i \neq j$). The amount of confidence transferred to the device O_j is a ratio of the confidence level associated to O_i and also depends on the proximity of both devices. Figure 2 illustrates this process. Sending this information could be a security problem in case of interception by an attacker or if the service is honest but curious. We propose a privacy protection scheme that enables user’s personal information protection and let the service compute the confidence level without knowing which type of information has been used for transparent authentication.

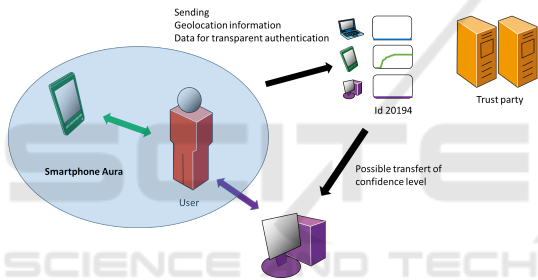


Figure 2: Illustration: The user’s smartphone has an Aura where the confidence is monitored by the trust party. If the computer is located in the smartphone Aura (not far in some sense), a part of the confidence level associated to the smartphone can be transferred to the computer one.

3.2 Privacy Protection

Privacy protection is a main and important issue to consider in our approach. As the verification process could be done by a trust party considered as honest but curious, a privacy protection of data coming from all devices is required. The concept of privacy protection of biometric data has been defined in 2001 in a seminal paper (Ratha et al., 2001). Since then, many methods have been proposed among random projections approaches (Pillai et al., 2010), BioHashing methods (Teoh et al., 2004), Bloom filters (Rathgeb et al., 2014), to cite just a few. The BioHashing algorithm is applied on biometric templates that are represented by real-valued vectors of fixed length (so the metric used to evaluate the similarity between two biometric features is the Euclidean distance). It generates binary templates of

length lower than or equal to the original length (here, the metric D_T used to evaluate the similarity between two transformed templates is the Hamming distance). This algorithm has been originally proposed for face and fingerprints by Teoh *et al.* in (Jin et al., 2004). Then, the BioHashing algorithm transforms the biometric template $T = (T_1, \dots, T_n)$ into a binary template $B = (B_1, \dots, B_m)$, with $m \leq n$ in Algorithm 1. A complete review of cancelable biometric systems can be found in (Patel et al., 2015).

More generally, a security analysis of the biometric system protecting the biometric template based on transformations (Rosenberger, 2018) are considered. The specificity of the BioHashing algorithm is that it uses a one way function and a random seed of m bits. It is important to note that every behavioral feature uses a different seed in order to create a specific BioCode. The performance of this algorithm is ensured by the scalar products with the orthonormal vectors. The quantization process of the last step ensures the non-invertibility of the data (even if $n = m$, because each coordinate of the input T is a real value, whereas the coordinates of the output B is a single bit). Finally, the random seed guarantees both the diversity and revocability properties.

Algorithm 1: BioHashing.

- 1: **Inputs**
- 2: $T = (T_1, \dots, T_n)$: biometric template,
- 3: K_z : secret seed
- 4: **Output** $B = (B_1, \dots, B_m)$: BioCode
- 5: Generation with the seed K_z of m pseudorandom vectors V_1, \dots, V_m of length n ,
- 6: Orthogonalize vectors with the Gram-Schmidt algorithm,
- 7: **for** $i = 1, \dots, m$ **do** compute $x_i = \langle T, V_i \rangle$.
- 8: **end for**
- 9: Compute BioCode:

$$B_i = \begin{cases} 0 & \text{if } x_i < \tau \\ 1 & \text{if } x_i \geq \tau, \end{cases}$$

where τ is a given threshold, generally equal to 0.

3.3 Process Service Description

Let’s consider a user U , having a number of devices n_d and a number of hotspots nh he/she defined a priori. A hotspot is a trusted area such as home or work place. This user has the possibility to register his/her devices and hotspots via an application provided by a trust party, by entering the IP address of each of possessed devices and the GPS coordinates of his/her hotspots. Once registered on this application, they

are considered as trusted devices and hotspots. The confidence on a hotspot (denoted by NAH) is variable and is set by the user. For example, in the case of a fully trusted hotspot (such as my home), NAH can be set to 100%. We suppose that the user has on each of its device a transparent authentication solution that allows a trust party to compute a confidence level guarantying that at any time, the device is used by the right user. A solution proposed by authors of (Guiga et al., 2020) could be used. This confidence level evolves with time i.e. the device sends at a set interval of time (as for example, each 3 minutes) some information (behavior, face biometric data...) to the trust service for the confidence computation. This confidence value decreases automatically by the trust party to ensure that if the device is not used by the legitimate user, it cannot be used by an impostor. In this work, we want at any time, to determine the trust level of each device by taking into account its Aura. This level can be increased based on belonging the trusted hotspots where the user and device are located.

For this purpose, we illustrate the process considering the following scenario. Let Alice be the user with 3 devices: a smartphone (S), a laptop (L) and an office computer (PC). In order to correctly authenticate herself to her devices, Alice uses passwords, either the same password for all 3 devices or different passwords for each device. In both cases, this authentication method is weak and vulnerable to different attacks. We wish to establish a connection between Alice's devices in order to allow the transfer a part of the confidence level on authentication from one to another device without Alice's intervention. Alice creates with her devices an authentication aura A. Let AO_1 be the smartphone aura, AO_2 the laptop aura and AO_3 the computer aura. Let A_T be Alice's Aura in trusted hotspots, in order to compute the confidence of Alice's device (the smartphone as for example), we first want to check if it belongs to A_T (i.e. if this device is in a trusted hotspot). We consider the confidence $C(O_i)$ of the device O_i calculated individually (not in the hotspot). We also define the confidence $C_H(O_i)$ of the device O_i belonging to a hotspot by the minimum of the sum of the confidence products of a device O_j (for any $i \neq j$) belonging to the same hotspot (having the trust NAH) and 100 (the maximal value of a confidence), given by the following equation:

$$C_H(O_i) = \min \left(\sum_{i \neq j}^{n_H} NAH \times C(O_j) + C(O_i), 100 \right) \quad (1)$$

With n_H the number of Alice's devices belonging to the same hotspot. This value is updated at each interval of time set by the trust service or user. We

assume that the initial confidence of a new device to which Alice wishes to authenticate is zero. In order to determine the possible transfer of confidence level among devices, we need to verify if they are located on the same hotspot. To achieve this goal, we can measure their geolocation using many data such as GPS coordinates, IP address or via the WIFI list. Let (g_1, g_2, \dots, g_n) be the geolocation data of Alice's smartphone. Then, to ensure the security and privacy of the geolocation data, we apply the BioHashing algorithm to generate a geolocation Biocode with Alice's secret key (here, a random seed value). In order to decide if the device is located in a known trusted hotspot, we compute the Hamming distance $dist_H$ between the Biocodes of the device geolocation data and the hotspot. The level of proximity to a hotspot is defined by the value of the Hamming distance. Among a decision threshold set by the trust party (risk management), the trust service can decide if the device is located in one of Alice's trusted hotspots. Note that the trust service is not able to know where is located this hotspot as it only knows its geolocation BioCode and do not know Alice's secret key. Figure 3, illustrates the adopted scenario.

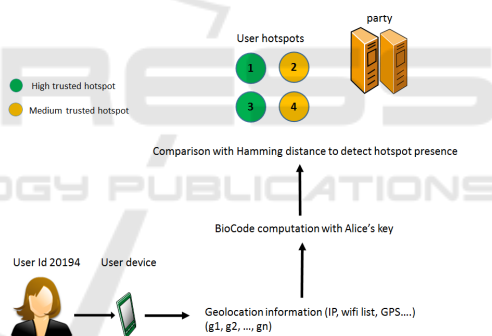


Figure 3: Illustration of the adopted scenario to determine the presence or not in a trusted hotspot.

For a number of devices $n_H = 2$, let's imagine a typical day in Alice's life described by the following scenario: Alice uses her smartphone every morning to read the news and consult her social networks, with the time spent logging on, her smartphone gains more confidence on authentication (transparent authentication). On her way to work, she continues to use her smartphone to call her mum. Now, when she arrives at her office, that has been previously declared as a high trusted hotspot, she wants to authenticate to her laptop. Having a sufficient level of confidence on her smartphone, she can use her laptop without the need for a re-authentication (transparent authentication gained with the confidence transferred from the smartphone). The confidence level $C_H(L)$ of her laptop can be calculated by the equation given

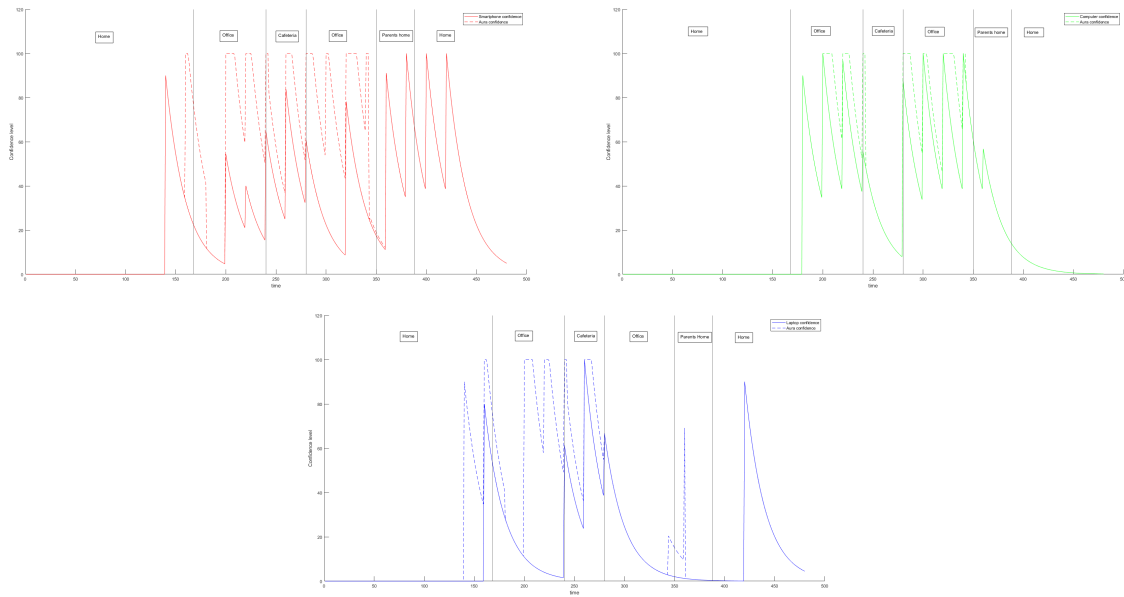


Figure 4: Alice’s Aura confidence evolution curve Vs Alice’s smartphone, Laptop and computer confidence evolution curve along a day.

below 2:

$$C_H(L) = \min (NAH \times C(S) + C(L), 100) \quad (2)$$

In case Alice uses her smartphone, but not enough to establish a confidence to be shared with other devices, another proof of authentication can be requested (a PIN code for example). We can see that, when trying to authenticate with a new device, we do not lose the confidence level already acquired on other devices in the Aura. So, initially, the new device gains the confidence of the whole Aura, whatever the type of hotspot. Note that the confidence associated to a device is updated at each interval of time, with the transfer from other devices (it could be at the previous time not equal to zero). In the next section, we illustrate the proposed method on simulated data.

4 ILLUSTRATIONS

In order to study the confidence evolution of Alice’s devices, We consider a specific scenario describing a typical day of Alice, mainly while using her smartphone, laptop and computer, where Alice has declared 4 trusted hotspots as following: Home(NAH=100), Office(NAH=90), Parents home(NAH=75), Cafeteria(NAH=50). We set in this illustration the natural decrease in the confidence level over time with an exponential decay (interval of time when data are sent to the trust party). We can consider figure 4 showing the impact

of the Privacy Authentication Aura solution on the confidence level of Alice’s devices, respectively on her smartphone, office computer and laptop vs the confidence level on Alice’s devices, along the day, in a transparent mono-device authentication context. We can clearly see that the Aura confidence curve is at least equal to the confidence curve of one device without applying the Aura solution. This is normal as defined in equation 1. In this work, we only considered the positive impact of the Aura on the confidence level on authentication of a device. Having other devices in the proximity or belonging to the same hotspot, leads to a higher confidence level, thanks to the transfer of confidence between devices. With this solution, we do not require another authentication request. Devices take benefit of the belonging to the same hotspot and of the transparent authentication acquired on one device. For example, we can see on figure 4, when Alice is in her office at t=170 (i.e. 8:30 am as we have 20 intervals per hour), the confidence level without the Aura solution is of 23% which is not considered enough to be authenticated, in case Alice wants to use her smartphone, another proof is requested. However, when using the Aura solution, we can see that the confidence level at t=170 is equal to 80%, which allows Alice to use her phone without any additional proof, thanks to the proximity with her computer and being in a trusted hotspot. Another example, when Alice goes to visit her parents, she has her laptop in her bag but she rarely use it, so at t=360, the

confidence level without the Aura concept is almost equal to zero. Yet, if she decides to use it, she has already gained on confidence level which increases to 69% when using the Aura solution by just being at her parents home which is declared as a trusted hotspot and by relying on the confidence on her smartphone over the time spent using it. In terms of privacy, the trust party, in order to authorize authentication, collects information to know whether a device is in a specific hotspot or not, but it is not allowed to know the content of data. In our case, the trust party has no right to have access to the geolocation data. It receives only the Biocodes *BG* because all collected data are protected by the Biohashing algorithm as mentioned in the section 3.2. So, the trust party can be informed of Alice's presence in a trusted hotspot without knowing exactly where she is. Noting that the mono-device transparent authentication privacy is respected as well, and we can refer to this work (Guiga et al., 2020) for more details.

5 CONCLUSION

We proposed in this paper a multidevices transparent authentication solution, called Privacy Authentication Aura, that improves the confidence level authentication comparing to a mono-device solution and ensures data privacy protection. A higher confidence is provided by the Aura when devices are located at the same trusted hotspot and it can be transferred from a device to another. It is true that in our process, the confidence decreases over time, but to keep transparency, it cannot be decreased abruptly, and, in fact, this can lead to intrusion attacks. Therefore, we aim to improve our process so the user can be alerted when one of her devices is not detected in the Aura but still have a high confidence. The user can decide to decrease the confidence of a device if it is not located in the same Aura. This process is classical to detect payment frauds (as for example, detecting a withdrawal of money in a foreign country), we plan to improve the proposed solution with a negative impact of the Aura on the authentication confidence level.

REFERENCES

- Cha, B.-R., Lee, S.-H., Park, S.-B., Ji, G.-K. L. Y.-K., et al. (2015). Design of micro-payment to strengthen security by 2 factor authentication with mobile & wearable devices. *Advanced Science and Technology Letters*, 109(7):28–32.
- Gonzalez-Manzano, L., de Fuentes, J. M., and Orfila, A. (2015). Access control for the cloud based on multi-device authentication. In *2015 IEEE Trustcom/BigDataSE/ISPA*, volume 1, pages 856–863. IEEE.
- Guiga, T., Rosenberger, C., and Schwartzmann, J.-J. (2020). When my behavior enhances my smartphone security. In *2020 International Conference on Cyberworlds (CW)*, pages 280–284. IEEE.
- Hajny, J., Dzurenda, P., and Malina, L. (2016). Multi-device authentication using wearables and iot. In *SECURITY*, pages 483–488.
- Hocking, C. G., Furnell, S. M., Clarke, N. L., and Reynolds, P. L. (2011). Authentication aura-a distributed approach to user authentication. *Journal of Information Assurance and Security*, 6(2):149–156.
- Jin, A. T. B., Ling, D. N. C., and Goh, A. (2004). Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern recognition*, 37(11):2245–2255.
- Juniper (2020). Juniper research press releases, "iot connections to reach 83 billion by 2024, driven by maturing industrial use cases". <https://www.juniperresearch.com/press/press-releases/iot-connections-to-reach-83-billion-by-2024-driven>. [Online; accessed 27-January-2021].
- Patel, V. M., Ratha, N. K., and Chellappa, R. (2015). Cancelable biometrics: A review. *IEEE Signal Processing Magazine*, 32(5):54–65.
- Pillai, J. K., Patel, V. M., Chellappa, R., and Ratha, N. K. (2010). Sectored random projections for cancelable iris biometrics. In *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*, pages 1838–1841. IEEE.
- Ratha, N. K., Connell, J. H., and Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal*, 40(3):614–634.
- Rathgeb, C., Breiting, F., Busch, C., and Baier, H. (2014). On application of bloom filters to iris biometrics. *IET Biometrics*, 3(4):207–218.
- Riva, O., Qin, C., Strauss, K., and Lymberopoulos, D. (2012). Progressive authentication: deciding when to authenticate on mobile phones. In *21st {USENIX} Security Symposium ({USENIX} Security 12)*, pages 301–316.
- Rosenberger, C. (2018). Evaluation of biometric template protection schemes based on a transformation. In *ICISSP*, pages 216–224.
- Teoh, A., Ngo, D., and Goh, A. (2004). Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern recognition*, 40.
- Xu, W. (2015). Mobile applications based on smart wearable devices. In *Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*, pages 505–506.
- Zhang, J., Wang, Z., Yang, Z., and Zhang, Q. (2017). Proximity based iot device authentication. In *IEEE INFOCOM 2017-IEEE Conference on Computer Communications*, pages 1–9. IEEE.