A Privacy-By-Design Architecture for Indoor Localization Systems*

Paolo Barsocchi[1 [0000−0002−6862−7593]], Antonello Calabrò[1 [0000−0001−5502−303X]], Antonino Crivello[1 [0000−0001−7238−2181]], Said Daoudagh[1,2 [0000−0002−3073−6217]], Francesco Furfari[1 [0000−0002−4957−828X]], Michele Girolami[1 [0000−0002−3683−7158]], and Eda Marchetti[1 [0000−0003−4223−8036]]

[1] CNR-ISTI, Pisa, Italy
[2] University of Pisa
{firstname.lastname}@isti.cnr.it

Abstract. The availability of mobile devices has led to an arising development of indoor location services collecting a large amount of sensitive information. However, without accurate and verified management, such information could become severe back-doors for security and privacy issues. We propose in this paper a novel Location-Based Service (LBS) architecture in line with the GDPR's provisions. For feasibility purposes and considering a representative use-case, a reference implementation, based on the popular Telegram app, is also presented. [3]

Keywords: Indoor localization systems · Location-based services · Access Control Systems · GDPR · Privacy-by-design

1 Introduction

The wide availability of mobile devices has led to an arising development of (indoor/outdoor) Location-Based Services (LBSs) for improving users' daily life and works. More specifically, a high number of stakeholders are exploiting such systems for providing commercial solutions, selling products, tracking facilities, social apps, and services. Most of the previously cited systems are supposed to acquire and store personal data such as IP address, the user's localization and the history of locations visited as well as a timestamp of such visits. As a result, the final users disseminate kinds of *digital crumbs* that might potentially disclose sensitive information without being aware of the actual risk.

Beyond Snowden [9] and the recent adoption in May 2018 of the General Data Protection Regulation (GDPR) [7], people sensitiveness about personal privacy, fortunately, has been increasing. However, in the context of Indoor Localization Systems (ILSs), there is still the missing of a standardized reference architecture that takes care of the security and privacy enforcement.

* Partially Supported by CyberSec4Europe Grant agreement ID: 830929.
[3] DA CONTROLLARE TUTTI GLI ORCID_IDs

In this paper we describe a novel LBS architecture in line with the GDPR provisions, i.e., able to strengthen the rights of individuals over their own data and to make organizations more accountable regarding the regulation. The provided solution relies on the innovative idea of integrating a GDPR-based Access Control (AC) system inside the localization architecture. We argue that the AC represents a promising technique for developing adequate and fine-grained mechanisms taking into account legal requirements, such as the data usage purpose, the management of the user's consents as well as enforcing the data retention period [4, 17, 18]. Thus, the main contribution of this paper is to schematize an Indoor Localization System (ILS) reference architecture. We define the purposes of the data management, the management of the user's consents, and the rights related to privacy and data protection correctly enforced so as to guarantee the privacy-by-design GDPR compliance.

To the best of our knowledge, our solution is the first proposal that integrates three key-aspects: i) the design of smart and easy-to-use ILS architecture, ii) the use of access control systems for resource and data management inside localization environment and, iii) the enforcement of the GDPR's provisions inside the localization systems.

This article is structured as follows: in the next section, an overview of background and related work is presented. Then, in Section 3 we describe the proposed privacy-by-design solution, while in Section 4, we present an application example. Finally, Section 5 concludes the paper.

2 Background and Related Work

In this section, we briefly describe the indoor localization, the GDPR, and the AC basic knowledge and their related works.

Considering the ILSs, their main peculiarities are the positioning and localization functionalities. Several proposals have been presented in the last decade for ILSs, each one showing differences, in terms of methods and data sources. Main ready to the market solutions are: IndoorAtlas [4], Indoor Google Maps and Anyplace [10]. Even if ILSs are a generally accepted cross-domain solution, they still lack of a generic standard architecture and, more importantly, they are agnostic about the privacy principles and exposed to the risk of location privacy violation [14].

The GDPR [7] defines *Personal Data* as any information relating to an identified or identifiable natural person called *Data Subject*. That means that a data subject is a Natural Person (a living human being), whose data are managed by a *Controller*. The GDPR is applied to the processing of personal data, whether it is automated (even partially) or not. It defines, among others, the following principles and demands: *Purposes*, i.e., data should only be collected for determined, explicit and legitimate purposes, and should not be processed later for other purposes; *Accuracy*, i.e., the processed data must be accurate and up-to-date regularly; *Retention*, i.e., data must be deleted after a limited period;

[4] https://www.indooratlas.com/

Subject explicit consent, i.e., data may be collected and processed only if the data subject has given his explicit consent.

Concerning the design of the AC, it is usually implemented through *Access Control Mechanism (ACM)*, which is the system providing a decision to an authorization request, typically based on predefined *Access Control Policy (ACP)*. The eXtensible Access Control Markup Language (XACML) [15] is one of the most widely used AC languages, and it provides the reference architecture in the AC environment. An XACML policy is a specific statement of what is and is not allowed, on the basis of a set of rules. Rules are defined in terms of conditions on attributes of subjects, resources, actions, and environment, and by combining algorithms for establishing the order among the existing rules.

Notwithstanding the importance of the role of AC systems, their integration with a localization system architecture is still an emerging topic [12]. Most of the results achieved so far have been focused either on: (1) using access control mechanisms for (physical) protection within virtual perimeters [11]; (2) using location information for automatically authenticate customer [13]; (3) on specific security attributes that do not fully cover the GDPR requirements [1, 5]. This paper enhances the current research by proposing, for the first time, a reference architecture that includes a location and topology-aware access control system to guarantee compliance with the GDPR provisions.

3 A privacy-by-design solution

In this section, we schematize the possible reference architecture for the indoor localization system which includes a GDPR-based AC system. The proposal extends and integrates the solutions presented in [8, 6, 3]. Figure 1 shows the main components of the proposed reference architecture that are:

User Agent (UA): the UA cooperates, on behalf of the user, with the indoor infrastructure to estimate the user's location. It is typically deployed in a smart device (e.g., smartphone, tablet or smartwatch). As shown in Figure 1, the UA is in charge of managing the user interaction for: automatically detecting the existence of an ILS (through the Discovery Service), enabling the localization of the device (through the Positioning Service); rendering the device position on a map (through the Mapping Service); managing the user's consents and sending/receiving access requests/responses (through the device GUI);

Localization Infrastructure (LI): the LI is an indoor distributed infrastructure in charge of determining the user's location. It relies on WiFi signals collected through the UA and it provides three main components: ① *Map Manager*, that manages the updating and storage of the internal maps; ② *Discovery Server*, that is in charge of sending the URL of the available ILSs to the different UA; ③; *Enhanced Indoor Localization System (E-ILS)*, that is the core component of LI and it relies on two databases for collecting the required information and personal data.

More specifically, the E-ILS is characterized by three main components: i) the *Communication and Interaction Orchestrator*, which is in charge of managing

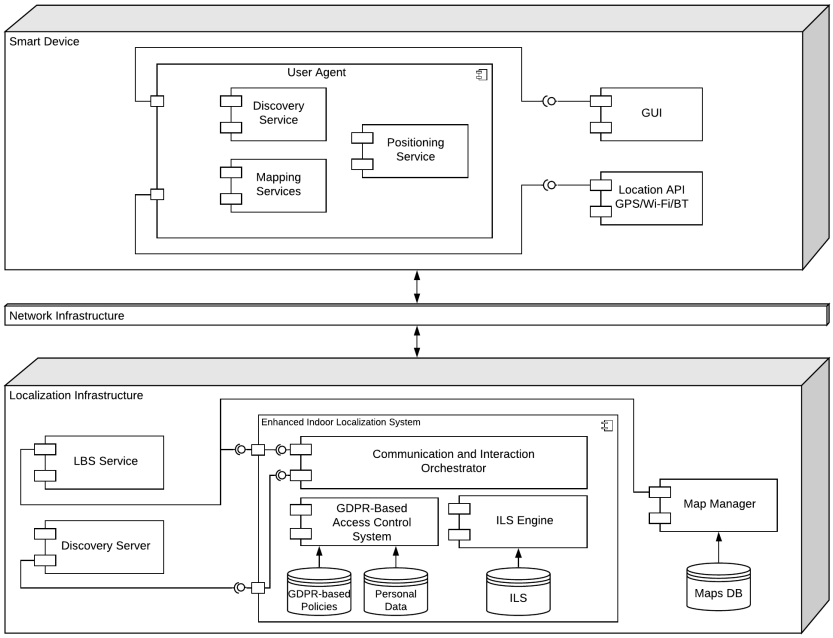

Fig. 1. The reference architecture: the UA implements the interaction between the users and the LI throughout a network infrastructure.

the communication to and from the E-ILS; ii) the *GDPR-Based Access Control System*, which rules the resources and data access; iii) the *ILS Engine*, which is in charge of estimating the User Agent's location. In turn, the *ILS Engine* returns back to the UA the timestamped coordinates, according to the map reference system (e.g., WGS84 reference system) [16].

The *ILS Engine* and the *GDPR-Based Access Control System* are designed to cooperate, since different people (e.g., the data owner, administrators or supervisors) and different services (e.g., booking services, advertisement services and navigation services) may ask the data access at different moments. More specifically, this last component is in charge of evaluating each single data access request and allowing or denying the access according to the collected consent, the data validity period, the specific users/service rights and the access control policies established inside the overall Localization Infrastructure. By extending the solution described in [2], the *GDPR-Based Access Control System* provides facilities for: 1. Gather privacy requirements from collected consents; 2. Identify privacy attributes; 3. Author the GDPR-based policies; 4. Test GDPR-based policies; 5. Deploy GDPR-based policies on the E-ILS; 6. Manage the data access. Through the interaction with the UA component, the *GDPR-Based Access Control System* provides facilities to perform steps from 1 to 4. Specifically, *GDPR-Based Access Control System* is in charge of preparing the consents to be subscribed by the users, extracting useful personal data from the signed con-

sents, and storing them into a secure and protect database. It also translates the consents first into processable structures, and then into enforceable GDPR-based access control policies so as to easily manage the GDPR provisions (we refer to [6, 3] for more details). In this paper we refer to XACML access control policies able to encode the GDPR principles for taking into account the users' consents. *GDPR-Based Access Control System* provides also facilities for validating the derived policies before storing them into the database. Finally, the *GDPR-Based Access Control System* is also in charge of managing access to the personal data during the online use of ILS (step 5 and 6 of the above list) by adapting and extending the current version of the XACML reference architecture (we refer to [6, 3] for more details).

4 Proximity Marketing: An Application Example

In this section the simple example of a *proximity marketing service* inside a mall is presented for describing the use of our proposal. In this use case, we suppose that infrastructure could provide several features such as: a navigation service for optimizing the path for completing a shopping list; a check-out management service notifying a user when to check-out; a discount notifier to advertise the user when he/she is in the proximity of a special offer and so on. Two relevant aspects need to be evaluated: i) the data collected during the user's localization might be used in order to improve the user-experience in a shopping mall (e.g., the optimal placement of products); ii) the appealing facilities of the indoor positioning can make available a set of personal data that can be misused and exploited in a way different than the users' expectations.

As an example of possible implementation, UA in Figure 1 has been implemented by extending the Telegram app [8]. In this case, the user starts the localization process by looking for the services available in the mall through the Telegram menu. Consequently, the UA retrieves information about the available localization infrastructures through a discovery service. This service performs a periodic Bluetooth/WiFi scan to retrieve information encoded in the payload of advertising messages of such technologies. In the current implementation, we encoded an URL on the payload of EddyStone beacons. In turn, the URL is used by the UA to retrieve the meta information of the ILS.

In the example of this section, the ILS engine implements the localization algorithm and the Map Server provides maps of the indoor environment. The localization algorithm leverages the WiFi signals received by the UA: it periodically scans the WiFi probes emitted by the WiFi Access Points (AP) in the nearby, and it analyzes the received signal strength (RSS) of the messages. The RSS collected from all the available WiFi APs are then transferred to the ILS, which analyzes them to estimate the device position. In turn, the ILS returns back the UA the timestamped coordinates so that to show on the map its current position. In our implementation, the user also receives through the UA GUI, a specific (textual) consent associated to the selected service, in which there is detailed information about the usage of personal data and their purpose such

as (i) who is the data owner; (ii) how the data will be processed, and for which purposes; (iii) the time of detention, and so on. In our proposal, according to the GDPR demands, the user's personal data, the device position, the timestamp as well as the ACPs area all kept on an exclusive database ruled by the *GDPR-Based Access Control System* (Figure 1). Moreover, the collected data are stored only for the time needed to provide the user with the required services.

Table 1. Example of Attribute Classification.

Identified Attribute	Attribute Category	GDPR Category	AC Category
Alice	Customer	Data Subject	Subject
Marketing Service	Service Provider	Controller	Subject
Read		Access	Action
Notification		Send	Action
Smart device ID	Biodata	Personal Data	Resource
GPS data	Biodata	Personal Data	Resource
Wi-Fi signal data	Biodata	Personal Data	Resource
On-board Sensors data	Biodata	Personal Data	Resource
Current Position	Location data	Personal Data	Resource
Shop Location	Location Data	Personal Data	Resource
Advertising	Purpose	Specific Purpose	Resource

As described in Section 3, the data extracted from *proximity marketing service* accepted consent are used for: automatically mapping the personal data into access control attributes, instantiating a rule for each structured representation and combining them into GDPR-based ACPs (we refer to [6, 3] for more details). As an example, considering the Art. 15.1 of the GDPR [5], Table 1 reports the mapping of the attributes for the following scenario: *Alice (Customer, i.e., Data Subject) provides the ID of her smart device, the GPS data, the WiFi signal data, and on-board sensors data. Such information are sent to the proximity marketing service (Controller) for advertising notifications when she is in proximity of a shop. Alice, at any time, can exercise her right of access pursuant the Art. 15.1.*

More precisely, column *Identified Attribute* of Table 1 contains the identified attributes; column *Attribute Category* shows their classification into a specific category; column *GDPR Category* maps attributes into regulation concepts; and finally, column *Access Control Category* maps to the access control entities. In Figure 2 the derived GDPR-based Access control policy written in XACML-like language is provided. Specifically, the policy is applicable to the subject *Alice* and contains two rules: (1) the first rule, with RuleId equal to *readRule*, represents the AC rule associated with Art. 15.1 and guarantees that Alice can read her provided personal information; (2) the second rule, called *defaultRule*, denies all which is not allowed explicitly.

[5] Art. 15.1 of the GDPR: 1. The data subject shall have the right to obtain [...] the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; [...] (Right of access by the data subject).

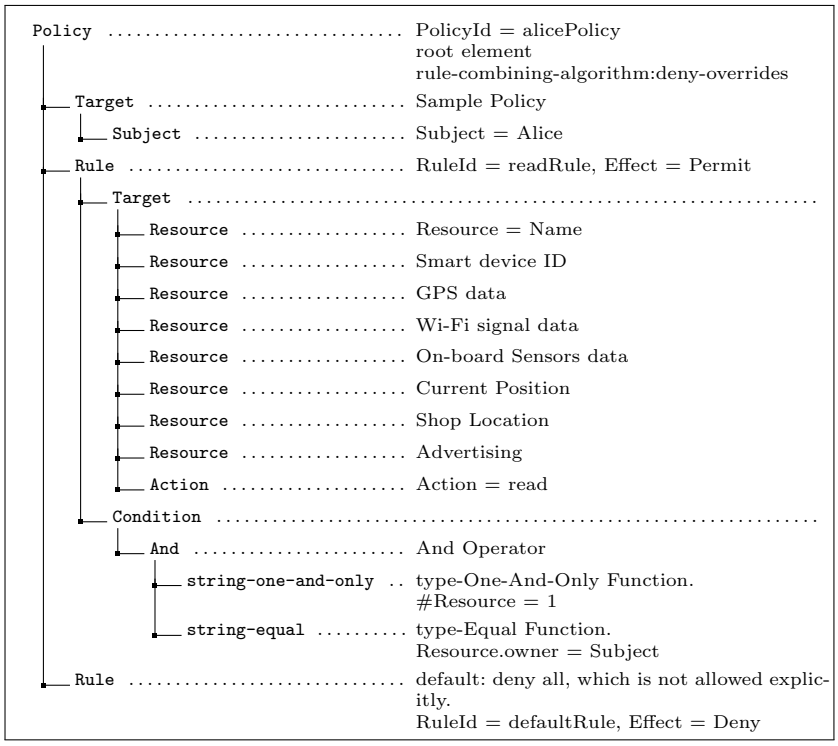

Fig. 2. Example of an XACML-like Policy.

5 Conclusions and Future Work

We present in this paper the architecture of an indoor localization able to guarantee the GDPR compliance through the integration of a specialized GDPR-based access control system. Our architecture replies to the users' need to be protected against unauthorized or unconscious privacy data collection and analysis. Indeed, according to the GDRP regulation, our privacy-preserving architecture can delegate to end-users the control of the provided personal data. We show the feasibility of our proposal by considering a proximity marketing service inside a mall. Even if very simple, the use case evidenced how the architecture could increase the privacy consciousness of end-users while they are using indoor environment services. By following this research line, we plan to extend our work with a real-world data collection campaign to evaluate the scalability of the platform at realistic conditions.

References

1. Barsocchi, P., Calabrò, A., Ferro, E., Gennaro, C., Marchetti, E., Vairo, C.: Boosting a low-cost smart home environment with usage and access control rules. Sensors **18**(6), 1886 (2018)

2. Bartolini, C., Daoudagh, S., Lenzini, G., Marchetti, E.: Gdpr-based user stories in the access control perspective. In: Proceedings of 12th QUATIC 2019, Ciudad Real, Spain, September 11-13, 2019, Proceedings. pp. 3–17 (2019)
3. Bartolini, C., Daoudagh, S., Lenzini, G., Marchetti, E.: Towards a lawful authorized access: A preliminary gdpr-based authorized access. In: Proceedings of ICSOFT 2019, Prague, Czech Republic, July 26-28, 2019. pp. 331–338 (2019)
4. Basin, D., Debois, S., Hildebrandt, T.: On purpose and by necessity. In: Proceedings of the Twenty-Second International Conference on Financial Cryptography and Data Security (FC) (February 2018)
5. Calabrò, A., Marchetti, E., Moroni, D., Pieri, G.: A dynamic and scalable solution for improving daily life safety. In: Proceedings of APPIS 2019. pp. 1–6 (2019)
6. Daoudagh, S., Marchetti, E.: A life cycle for authorization systems development in the GDPR perspective. In: Proceedings of the Fourth Italian Conference on Cyber Security (ITASEC), Ancona, Italy, February 4th to 7th, 2020. pp. 128–140 (2020)
7. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union **L119**, 1–88 (May 2016)
8. Furfari, F., Crivello, A., Barsocchi, P., Palumbo, F., Potortì, F.: What is next for indoor localisation? taxonomy, protocols, and patterns for advanced location based services. In: Proceedings of IPIN 2019. pp. 1–8. IEEE (2019)
9. Gellman, B., Gribbons, J.M.: Edward snowden says motive behind leaks was to expose surveillance state. (2013)
10. Georgiou, K., Constambeys, T., Laoudias, C., Petrou, L., Chatzimilioudis, G., Zeinalipour-Yazti, D.: Anyplace: A crowdsourced indoor information service. In: Proceedings of CMDM 2015. vol. 1, pp. 291–294. IEEE (2015)
11. Greaves, B., Coetzee, M., Leung, W.S.: Access control requirements for physical spaces protected by virtual perimeters. In: Furnell, S., Mouratidis, H., Pernul, G. (eds.) Trust, Privacy and Security in Digital Business. pp. 182–197. Springer International Publishing, Cham (2018)
12. Greaves, B., Coetzee, M., Leung, W.S.: A comparison of indoor positioning systems for access control using virtual perimeters. In: Fourth International Congress on Information and Communication Technology - ICICT 2019, London, UK, February 25-26, 2019, Volume 1. pp. 293–302 (2019)
13. Haofeng, J., Xiaorui, G.: Wi-fi secure access control system based on geo-fence. In: Proceedings of ISCC 2019. pp. 1–6 (2019)
14. Konstantinidis, A., Chatzimilioudis, G., Zeinalipour-Yazti, D., Mpeis, P., Pelekis, N., Theodoridis, Y.: Privacy-preserving indoor localization on smartphones. IEEE Transactions on Knowledge and Data Engineering **27**(11), 3042–3055 (2015)
15. OASIS: eXtensible Access Control Markup Language (XACML) Version 3.0. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html (January 2013)
16. Potortì, F., Crivello, A., Girolami, M., Barsocchi, P., Traficante, E.: Localising crowds through wi-fi probes. Ad Hoc Networks **75**, 87–97 (2018)
17. Ramadan, Q., Salnitriy, M., Strüber, D., Jürjens, J., Giorgini, P.: From secure business process modeling to design-level security verification. In: Proceedings of MODELS 2017. pp. 123–133. IEEE (September 2017)
18. Ranise, S., Siswantoro, H.: Automated legal compliance checking by security policy analysis. In: Proceedings of SAFECOMP 2017. LNCS, vol. 10489, pp. 361–372. Springer (2017)