DEMO: CoIoT: A Consent and Information assistant for the IoT

Mathieu Cunche
mathieu.cunche@insa-lyon.fr
Univ Lyon, INSA Lyon, Inria, CITI
Villeurbanne, France

Daniel Le Métayer
daniel.le-metayer@inria.fr
Univ Lyon, Inria, INSA Lyon, CITI
Villeurbanne, France

Victor Morel
victor.morel@inria.fr
Univ Lyon, Inria, INSA Lyon, CITI
Villeurbanne, France

ABSTRACT

The Internet of Things (IoT) raises specific issues in terms of information and consent, which makes the implementation of the General Data Protection Regulation (GDPR) challenging in this context. In this demo paper, we propose a prototype implementation of a consent and information assistant for the IoT coined CoIoT. This assistant is presented as an Android application called a Personal Data Custodian (PDC), working with devices called BLE Privacy Beacons. CoIoT enables the automatic communication of information about personal data collection, as well as a seamless management of consent to personal data collection.

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; *Usability in security and privacy*.

KEYWORDS

privacy, IoT, information, consent, GDPR, regulation.

ACM Reference Format:
Mathieu Cunche, Daniel Le Métayer, and Victor Morel. 2020. DEMO: CoIoT: A Consent and Information assistant for the IoT. In *13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '20), July 8–10, 2020, Linz (Virtual Event), Austria.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3395351.3401797

1 CONTEXT

The development of the Internet of Things (IoT) raises specific privacy issues especially with respect to information and consent. People are generally unaware of the devices collecting data about them and do not know the organizations operating them. Solutions such as stickers or wall signs are not effective information means in most situations. As far as consent is concerned, individuals do not have simple means to express and communicate it to the entities collecting data. Furthermore, the devices used to collect data in IoT environments have scarce resources; some of them do not have any user interface, are battery-operated or operate passively (they collect data without emitting any signal).

In Europe, the General Data Protection Regulation (GDPR) [2] puts emphasis on the control of data subjects over their personal data. As far as transparency is concerned, the GDPR defines the categories of information to be provided to data subjects: identity of the controller, purpose of the processing, categories of personal data concerned, recipients, etc. The GDPR also defines a number of conditions for the validity of consent: it should be freely given, specific, informed and unambiguous. Its application to the IoT is not obvious though.

We devised in [1] a generic framework in line with the GDPR addressing these information and consent issues in the IoT. In this demo paper, we present more specifically the prototype implementation of an assistant instantiating the framework. The prototype is protective both for data subjects (persons from whom data is collected, following the GDPR terminology, hereinafter "**DS**") and for data controllers (entities collecting data, following the GDPR terminology, hereinafter "**DC**"). We assume that DC deploy devices that can collect different types of personal data and/or communicate information to DS. For their part, DS may own several devices and at least one of them (typically a smartphone) can be used to consult the information provided by DC and to express their consent. We call this device the **Gateway Device**. We use the expression "**DS privacy policy**" to refer to the choices of the data subject regarding his personal data and "**DC privacy policy**" to refer to the privacy policy declared [1] by a DC.

2 PROTOTYPE IMPLEMENTATION AND EVALUATION

In this section, we briefly describe our prototype implementation of an assistant addressing the issues aforementioned.

2.1 Implementation

2.1.1 Setup. We use beacons called **BLE Privacy Beacons** combined with a mobile application called a Personal Data Custodian (**PDC**) running on an Android phone. The BLE Privacy Beacon is based on a low cost (less than $6) hardware (*Espressif ESP32* [2]) that implements the information and consent mechanisms (the code of the BLE Privacy Beacon and PDC are available online[3]). We have implemented a prototype tracking system monitoring Bluetooth signals and storing MAC addresses and timestamps. The tracking system is augmented by BLE Privacy Beacons and a consent management mechanism that discards data for which consent has not been obtained. The PDC can also manage consent of other devices owned by a DS. Here, another DS device is a Garmin forerunner 235 smartwatch. A sketch of this implementation is pictured in Figure 1.

2.1.2 Functioning. The mobile application acts as an assistant and enables the definition of DS privacy policies in a user-friendly manner. DS can add, update and delete rules through a scroll-down

WiSec '20, July 8–10, 2020, Linz (Virtual Event), Austria

ACM ISBN 978-1-4503-8006-5/20/07.
https://doi.org/10.1145/3395351.3401797

[1] A declaration can be seen as a commitment of the DC to implement his DC privacy policy but the actual enforcement of this policy is outside the scope of this paper.
[2] https://www.espressif.com/en/products/hardware/esp32/overview
[3] Respectively at https://github.com/cunchem/BLE_Privacy_Beacon.git and https://gitlab.inria.fr/vmorel/coiot

menu. The PDC can also instantiate generic consents, i.e., consents for a category of type of data. For instance, the PDC can instantiate *Identifiers* instead of atomic values such as *Bluetooth MAC address* and *Wi-Fi MAC address*. The Privacy Beacons broadcast their 86 bytes long DC privacy policy, taking advantage of the *Advertising* features of the BLE protocol. Upon reception, the DC policy is compared with the current DS policy, and the Gateway Device issues a consent message in case of compliance. The consent is sent through the Attribute Protocol. The consent message comprises the identifiers of DS devices — including the MAC address of the smartwatch — as well as a hash of the DC privacy policy to which the DS consents. Once the consent has been retrieved by the DC Privacy Beacon, it is stored by the tracking system. For each collected data item, the system checks whether a consent has been collected for this device identifier (in our case, a Bluetooth MAC address). Data is stored only if it is the case.

2.1.3 Additional feature: negotiation. If the DC policy does not comply with the DS policy, the Gateway Device and the Privacy Beacon undertake a negotiation. A negotiation consists in: 1) communicating the DS policy from the Gateway Device to the DC Privacy Beacon, 2) computing the terms on which the two policies agree, 3) communicating a new DC policy from the DC Privacy Beacon to the Gateway Device if the DC agrees to the more restrictive terms laid by the DS. The Gateway Device then issues a consent to the new DC policy which we assume to be compliant with the DS policy by construction.

2.1.4 Additional feature: registry. In addition to peer-to-peer communications with BLE Privacy Beacons, the PDC can also retrieve information from a distant server called a **registry**. A registry is a database freely accessible through the Internet, storing all relevant information about DC devices, including the DC policies. Communications through DC registries have several advantages compared to BLE Privacy Beacons: (1) they enable the visualization of DC policies regardless of the location of DS, which means that DS can be informed about the collection of data before visiting an area and (2) they provide a flexible management approach for DC policies – they do not require a specific infrastructure or particular capabilities of the devices except for an Internet connection. [4]

2.2 Evaluation

Even if the prototype presented here does not intend to be production-ready, it is fully functional and it addresses the issues raised in Section 1. In the following, we assess the strengths and limitations of the prototype with respect to the communication of information to DS, and with respect to the management of consent.

2.2.1 Information.

- The declaration by DC of their devices is performed by the Privacy Beacons.
- The range of the collecting devices can be tuned to fit with the range of Privacy Beacons to ensure that any DS about whom personal data can be collected receives the declaration sent by the DC. In practice, DC privacy policies are retrieved between one and five seconds after the PDC enters the area.

[4]Therefore, they can be well-suited to passive devices such as cameras.

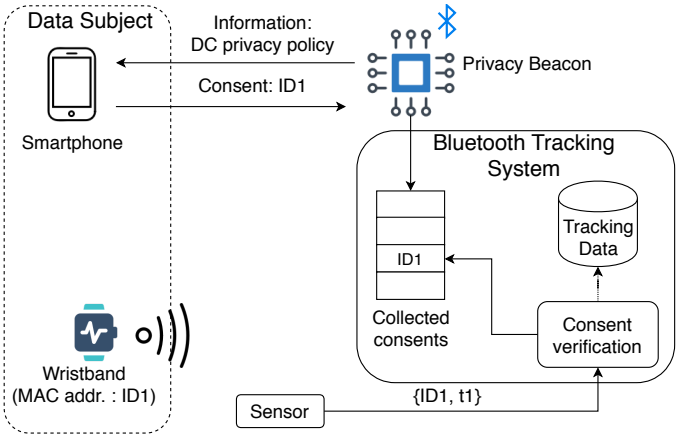

Figure 1: Illustration of the Bluetooth tracking scenario. The DS is informed of a tracking system between his Gateway Device (smartphone) and the Privacy Beacons. Communication between the smartphone and the Privacy Beacons happens over BLE. Depending on the DS policy, the Gateway Device sends a consent to the Privacy Beacon, undertakes a negotiation, or ignores this DC policy from now on. If a consent is received, it is securely stored by the tracking system. If a negotiation is undertaken, the DS policy is sent (more details in Section 2.1.3). When in range of sensors, the Bluetooth MAC addresses of the wristband and of the Gateway Device are passively collected and only stored if a consent has been retrieved; the MAC addresses are immediately deleted otherwise.

- This information is presented to the DS on the PDC. The presentation highlights information of interest to the DS, such as the type of data collected and the retention time. In the next version of the prototype, the presentation will also include a link to the full DC privacy policy.

2.2.2 Consent.

- The PDC makes it possible for DS to define, modify and delete privacy policy rules. These rules express the conditions under which DS consent to the collection of their data. Consent are communicated along a hash of the DC policy to ensure their integrity and authenticity.
- DC receive the consents through Privacy Beacons. When consent is not received, the personal data is immediately deleted.
- DC can store the consents on a central server through Privacy Beacons. Consents are stored on a secure ledger to ensure their integrity, using the implementation of Merkle Hash Trees by Ogden et al [3].

As far as costs are concerned, the prototype demonstrates that communication of information and consent management can be instantiated in real life use cases with a low-cost implementation.

3 CONTENT OF THE DEMONSTRATION

The demonstration is a video presenting features of CoIoT in different scenarios. Note that the retrieval of DC policies from a registry is not showed here.

A DS configures her DS policy on her PDC. She visualizes the DS policy, add a new rule, and modify another rule. The DS policy used addresses different DC and types of data (see Figure 2). Only the relevant rules are considered in the scenarios. She bonds her smartwatch to the PDC: this other DS device is not endowed with a screen large enough to permit user-friendly interactions, but the PDC now manages a DS policy encompassing the two devices.

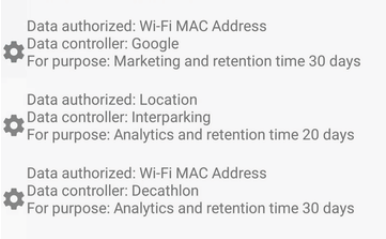

Figure 2: DS policy used in our setup.

We consider a setup where a DC deploys a device to track DS using BLE. The DC device is a Privacy Beacon able to declare its DC policy, to retrieve consent, and to undertake a negotiation. The Privacy Beacon continuously broadcasts the DC policy through BLE. The DC is a fictitious company called Interparking, its DC policy requests location data for different purposes. The tracking system is technically able to track the DS, but the DC device immediately discards data prior to any communication of consent.

The DS enters the range of collection of the DC device. Because the tracking and the communication technology are identical, namely BLE, the range of collection is equivalent to the range of communication. The PDC on the Gateway Device detects the Privacy Beacon, and retrieves its DC policy (see Figure 3). The PDC compares the DC policy with the DS policy in store. Upon comparison of the two policies, we propose four different scenarios.

In a first scenario, the commitment stated in the DC policy complies with the requirements stated in the DS policy: the PDC issues a consent to the Privacy Beacon (see Figure 4).

In a second scenario, the DC policy does not comply with the DS policy at first. The DS did not consider these terms before, but modify her DS policy to comply with the DC policy. The PDC then issues a consent to the Privacy Beacon.

In a third scenario, the DC policy does not comply with the DS policy at first. The DS does not want to modify her DS policy, but the two policies possess common terms, i.e., the DS agrees to data collection for analytics purposes only. As a result, the two devices undertake a negotiation: 1) the Gateway Device communicates the DS policy to the Privacy Beacon, 2) the Privacy Beacon computes the terms on which the two policies agree, 3) the Privacy Beacon has been programmed to accept these new terms, and sends the new DC policy in unicast to the Gateway Device, 4) the new DC policy is compliant with the DS policy by construction, the Gateway Device issues a consent for the new DC policy.

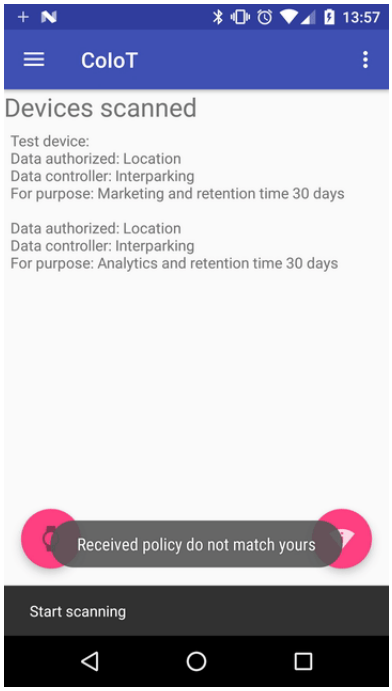

Figure 3: Scan of Privacy Beacon

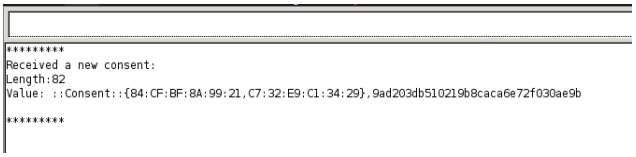

Figure 4: Reception of consent on a Privacy Beacon

In a fourth scenario, the DC policy does not comply with the DS policy. The DS does not agree to any term of processing proposed by the DC policy. The PDC ignores this DC policy from now on.

Any consent received is stored in a secure ledger.

ACKNOWLEDGMENTS

This work has been partially funded by the CHIST-ERA project UPRISE-IoT (User-centric Privacy and Security in the IoT) and the ANR project CISC (Certification of IoT Secure Compilation).

REFERENCES

[1] V. Morel, M. Cunche, and D. Le Métayer. 2019. A Generic Information and Consent Framework for the IoT. In *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. 366–373.

[2] Official Journal of the European Union. 2016. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

[3] Maxwell Ogden, Karissa McKelvey, Mathias Buus Madsen, and Code for Science. [n.d.]. Dat - Distributed Dataset Synchronization And Versioning. https://doi.org/10.31219/osf.io/nsv2c