DEMO: Venom: a Visual and Experimental Bluetooth Low Energy Tracking System

Guillaume Celosia, Mathieu Cunche

DEMO: Venom: a Visual and Experimental Bluetooth Low Energy Tracking System

Guillaume Celosia
Univ Lyon, INSA Lyon, Inria, CITI
F-69621 Villeurbanne, France
guillaume.celosia@insa-lyon.fr

Mathieu Cunche
Univ Lyon, INSA Lyon, Inria, CITI
F-69621 Villeurbanne, France
mathieu.cunche@insa-lyon.fr

ABSTRACT

The Bluetooth Low Energy (BLE) protocol is being included in mobile devices such as smartphones, headphones and smartwatches. As part of the BLE service discovery mechanism, devices announce their presences by broadcasting radio signals called advertisement packets that can be collected with off-the-shelf hardware and software. To avoid the risk of tracking based on those messages, BLE features an address randomization mechanism substituting the device MAC address with random temporary pseudonyms. However, the payload of advertisement packets still contains fields that can negate the randomization mechanism by exposing static identifiers.

In this paper, we present *Venom* (*Visual and ExperimeNtal BluetOoth Low Energy tracking systeM*), an experimental tracking platform aiming to raise public awareness about physical tracking technologies and experiment privacy-preserving mechanisms. *Venom* tracks users by collecting advertisement packets broadcasted by their BLE-enabled devices, and displays related information.

CCS CONCEPTS

• **Networks** → **Network privacy and anonymity**; • **Security and privacy** → *Mobile and wireless security*.

KEYWORDS

Privacy; Bluetooth Low Energy; Tracking; Address randomization; Internet of Things.

ACM Reference Format:
Guillaume Celosia and Mathieu Cunche. 2020. DEMO: Venom: a Visual and Experimental Bluetooth Low Energy Tracking System. 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/10.1145/3395351.3401696

1 INTRODUCTION

Bluetooth Low Energy (BLE) has been adopted for battery-powered devices such as smartphones, headphones and smartwatches. According to the Bluetooth Special Interest Group (SIG), more than 3 billion devices supporting BLE have been shipped in 2019 [9].

While radio technologies such as Bluetooth/BLE or Wi-Fi bring hands-on facilities, they also have the potential to expose users to privacy threats. In digital technologies, physical tracking and user activity monitoring are common things where such technologies allow to detect, recognize and categorize human activities [4, 7]. Sets of sensors are leveraged by radio-based tracking systems and collect identifiers contained in signals emitted by radio-enabled devices. Those identifiers are then processed to detect the presence of users and estimate their mobility.

Because BLE is included in a wide range of mobile devices, it is exploited by the physical tracking industry [5]. To protect users against tracking, the Bluetooth Core Specification [8, Vol 3, Part C, sec. 10.7] defines the use of temporary link layer identifiers that periodically change for a random value. However, it has been shown [3] that users can still be tracked because of static identifiers found within radio signals broadcasted by their devices.

As other wireless technologies, BLE embeds an advertising mechanism [8, Vol 3, Part C, sec. 11] providing a means to discover nearby devices with their characteristics and services. To enable this discovery mechanism, BLE devices periodically broadcast advertisement packets that are populated with a variety of cleartext information.

Despite efforts from both the industry and data protection authorities, the privacy of users is still in jeopardy [1]. In addition, the fact that tracking technologies are not well known by the general public aggravates the situation. As a consequence, the purpose of this work is to raise public awareness towards physical tracking systems, and especially about tracking issues implied by the advertising mechanism of BLE devices.

To this end, we implemented *Venom*, a *Visual and ExperimeNtal BluetOoth Low Energy tracking systeM*. As opposed to *Wombat* [6], its counterpart applied to the Wi-Fi technology, *Venom* leverages a wireless infrastructure to track users through their BLE-enabled mobile devices (e.g. smartwatches). Used for demonstrational purposes, we also augmented this system with a privacy-enhancing feature based on the vicinity, and allowing users to seamlessly express their dissent to the tracking.

2 THE VENOM TRACKING SYSTEM

Venom is a BLE tracking system supporting collection, storage and processing of advertisement packets. Those features are implemented over a distributed wireless infrastructure composed of:

- Clients: wireless monitoring-capable devices that collect advertisement packets and forward them to the broker;
- Broker: receives data from clients, stores and processes them (parse advertisement packets, analyze advertising data, etc.) in a local database.

To collect advertisement packets, *Venom* only requires Bluetooth cards supporting the BLE protocol. This is the case for most off-the-shelf Bluetooth cards on computers running a Unix-like system. To enable communication between clients and the broker, the *Venom* tracking system relies on its own custom Wi-Fi network. Finally, the advertisement packets parser has been built from the online official Bluetooth SIG resources, third-party public resources[1] and the

[1]The *advlib* advertisement packet decoding library, the *RaMBLE* Android mobile application and the *bleah* BLE scanner tool.

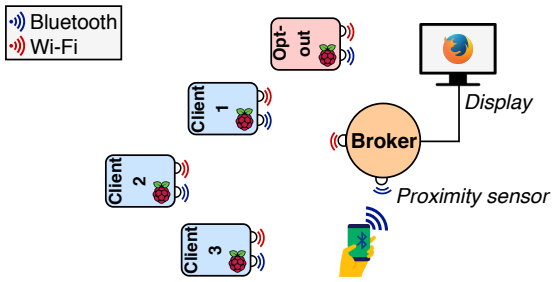

Figure 1: Architecture of the *Venom* tracking system.

reverse engineering of the *Apple* Continuity, *Microsoft* Connected Devices Platform and *Google* Nearby proximity protocols [2].

In addition to its principal features, we enriched *Venom* with a user interface along with an opt-out client:

- User interface: displays information about tracked devices through proximity detection[2]. Note that, the interface has been made to address as much types of audiences as possible (the general public, industrials, researchers and students);
- Opt-out client: implements a basic opt-out mechanism for users that do not want to be tracked by the system.

Figure 1 presents the architecture of *Venom*. It features core functionalities of industrial Bluetooth/BLE tracking systems: device detection, identification and itinerary tracking. We assume that those functionalities are enough to present principles of radio-based tracking systems, and to initiate discussions on corresponding privacy issues.

Information captured by the system are only data contained in advertisement packets sent by BLE devices having an enabled Bluetooth interface. Traffic data from associated devices, timing or physical-layer information are not considered. The display includes metadata of the advertisement packet (device addr., type of addr., etc.), a list of extracted information along with an inference of the device type based on its advertised device name.

To minimize privacy risks for users, we keep as little necessary information as possible. In particular, collected data of a participant are kept for a maximum of 15 minutes after its departure. Furthermore, *Venom* only detects devices in close range[3] of antennas to ensure that only volunteering participants will have their data collected and processed.

3 PRIVACY-PROTECTION FEATURE

Most tracking systems collect data of users without their consents. Therefore, to bring users possibilities to escape tracking, opt-out mechanisms have been deployed. Generally, such mechanisms involve a webpage on which the user has to declare its device MAC address. However, this approach presents usability issues preventing users from protecting their privacy through opt-out mechanisms.

In this work, we leverage BLE core elements to transmit the opt-out decision. In fact, we implemented a usable opt-out mechanism to which a device, whose owner wants to opt out, only has to be close to the `Opt-out` Bluetooth antenna of *Venom*. Note that, this differs from the opt-out mechanism introduced in [6], with which Wi-Fi devices willing to opt out must associate to an access point. Finally, upon this event, the tracking system will learn the device MAC address by parsing received nearby advertisement packets.

[2]Nearby devices are detected using the Received Signal Strength Indication (RSSI).
[3]A few centimeters.

4 INTERACTION WITH PARTICIPANTS

During the demonstration, visitors discovering the exhibition are tracked leveraging advertisement packets broadcasted by their carried BLE devices. At the entry, they are informed of the presence of the tracking system and the opt-out mechanism. By bringing their device close to the `Report` Bluetooth antenna of *Venom*, they are able to test the information collected from their devices. A comprehensive analysis of the collected data (identifier, brand of the device, etc.) along with an approximate representation of the user itinerary inside the exhibition is then displayed on a screen as a feedback to the participant (see Figure 2).

5 CONCLUSION

We introduced *Venom*, an experimental tracking system to shed light on privacy issues of BLE-enabled devices. We showed how it can be used for demonstrational purposes to raise user awareness about radio-based physical tracking technologies. We also explained how this platform can be leveraged as a basis to develop and test privacy-preserving mechanisms. To this end, we presented a BLE-based opt-out mechanism that does not involve any action from users on their devices, unlike the one proposed in *Wombat* [6].

Beyond public awareness, the objective of *Venom* is to point out the necessity to complement the Bluetooth Core Specification with additional requirements that would cover privacy issues on the BLE protocol, and especially on the advertising mechanism. Indeed, specifications do not provide any guidelines about the content of the advertising payload regarding physical tracking implications.

ACKNOWLEDGEMENTS

This work was supported by the INSA Lyon - SPIE ICS IoT chair and the H2020 SPARTA Cybersecurity Competence Network project.

REFERENCES

[1] Johannes K Becker, David Li, and David Starobinski. 2019. Tracking anonymized bluetooth devices. *Proceedings on PETS* 2019, 3 (2019).
[2] Guillaume Celosia and Mathieu Cunche. 2019. Saving Private Addresses: An Analysis of Privacy Issues in the Bluetooth-Low-Energy Advertising Mechanism. In *Proceedings of EAI MobiQuitous*.
[3] Kassem Fawaz, Kyu-Han Kim, and Kang G Shin. 2016. Protecting privacy of BLE device users. In *USENIX Security Symposium*.
[4] Taher Issoufaly and Pierre Ugo Tournoux. 2017. BLEB: Bluetooth Low Energy Botnet for large scale individual tracking. In *NextComp*. IEEE.
[5] Libelium. 2019. Detecting iPhone and Android Smartphones by WiFi and Bluetooth. (2019). http://www.libelium.com/products/meshlium/smartphone-detection
[6] Célestin Matte and Mathieu Cunche. 2017. Wombat: An experimental wi-fi tracking system.
[7] ABM Musa and Jakob Eriksson. 2012. Tracking unmodified smartphones using wi-fi monitors. In *Proceedings of ACM SenSys*.
[8] Bluetooth SIG. 2019. *Bluetooth Core Specification v5.2.* https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=478726
[9] Bluetooth SIG. 2020. *2020 Bluetooth Market Update.* Technical Report. https://www.bluetooth.com/wp-content/uploads/2020/03/2020_Market_Update-EN.pdf

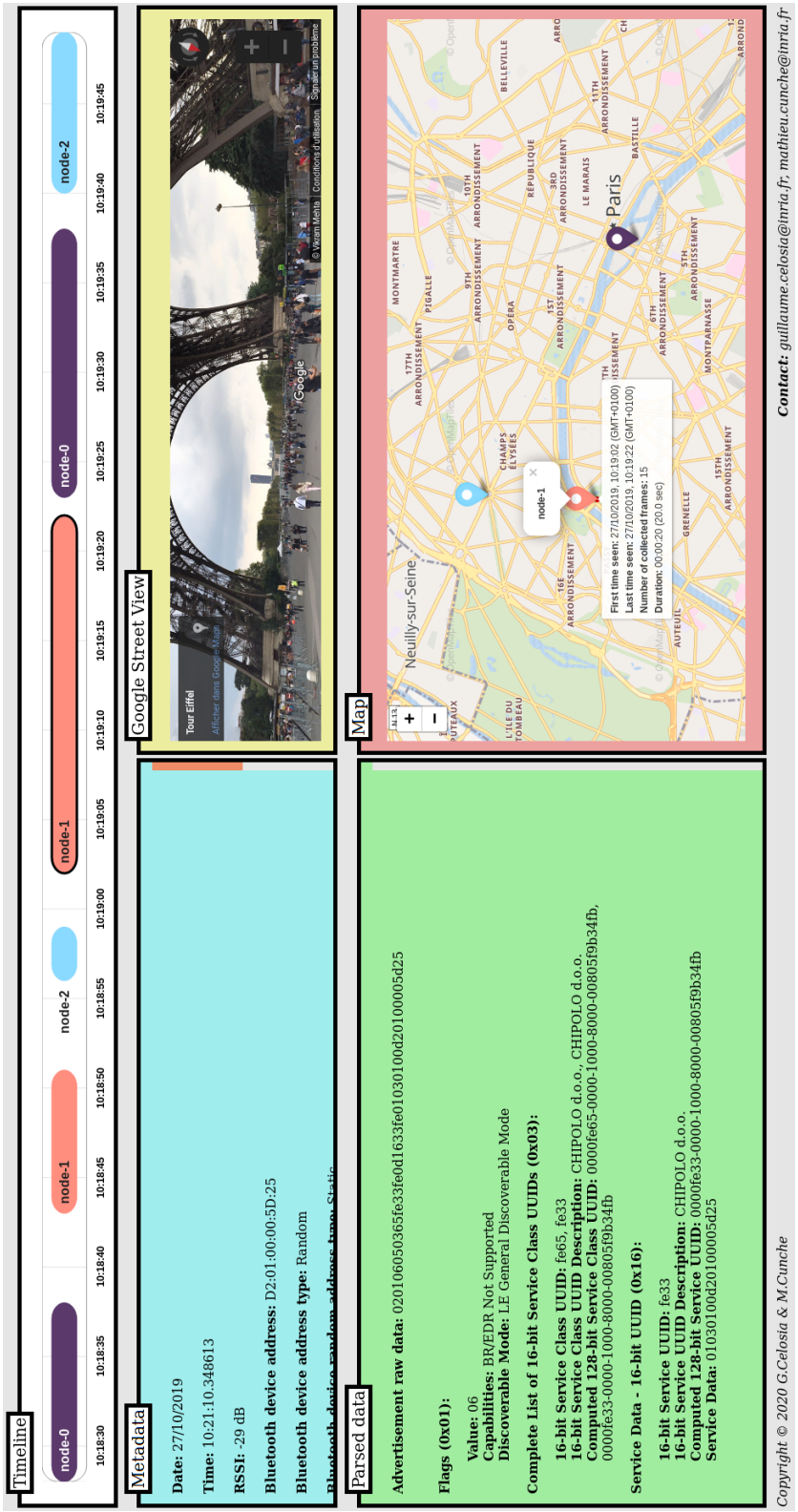

Figure 2: Example output of a *Chipolo Classic* BLE keyring device.