DEMO: Himiko: A human interface for monitoring and inferring knowledge on Bluetooth-Low-Energy objects

Guillaume Celosia, Mathieu Cunche

DEMO: Himiko: A Human Interface for Monitoring and Inferring Knowledge on Bluetooth-Low-Energy Objects

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 a growing number of connected objects such as smartphones, fitness trackers, headphones and smartwatches. As part of the service discovery mechanism of BLE, devices announce themselves 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 that substitutes the device MAC address with random temporary pseudonyms. However, the payload of the advertisement packet still contains fields that can hamper the randomization mechanism by exposing counters and static identifiers. In addition to defeating the randomization mechanism, some of these fields can leak sensitive attributes of the owner such as his medical condition.

As a consequence, we implemented *Himiko* to raise awareness about the privacy issues that the BLE advertising mechanism can involve. This tool aims to show the information that a passive eavesdropper can infer by leveraging the contents of BLE advertisement packets. The advertising raw data are collected and processed from devices that have their Bluetooth interface enabled. The user is then shown the information that are leaking from his device.

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. 2019. DEMO: Himiko: A Human Interface for Monitoring and Inferring Knowledge on Bluetooth-Low-Energy Objects. In *WiSec '19: ACM Conference on Security and Privacy in Wireless and Mobile Networks, May 15–17, 2019, Miami, FL, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3317549.3326297

1 INTRODUCTION

Bluetooth Low Energy (BLE) has been adopted for devices with low energy resources such as smartphones, fitness trackers, headphones and smartwatches. According to the Bluetooth Special Interest Group (SIG), more than 2 billion devices supporting BLE have been shipped in 2017 [1].

While wireless technologies such as Bluetooth/BLE or Wi-Fi bring hands-on facilities, they also have the potential to expose users to privacy threats. For instance, users can be subject to physical tracking because of the identifiers found within the radio signals emitted by their devices [4, 7, 8]. To protect users against this threat, the Bluetooth Core Specification [6, Vol 3, Part C, sec. 10.7] defines the use of temporary link layer identifiers that periodically change for a random value. Despite this improvement, it has been shown [3, 4] that some information can still leak from BLE devices.

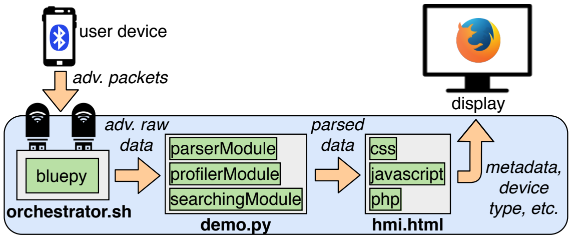


Figure 1: Architecture of the system.

As other wireless technologies, BLE embeds an advertising mechanism [6, Vol 3, Part C, sec. 11] that provides a means to discover nearby devices along with their characteristics and available services. To enable this discovery mechanism, BLE devices periodically broadcast advertisement packets that are populated with a variety of cleartext information.

In addition to tracking [5], advertisement packets include data that can reveal the type of the device [2], exposing the user to inventory attacks and inference of sensitive attributes. For instance, some medical devices are broadcasting their types (hearing aid, insulin pen, etc.) trivially betraying a medical condition of the owner.

The *Himiko* tool extends those works by capturing and processing in real-time the content of advertisement packets. Based on online official Bluetooth SIG resources[1] along with recent research findings [2], we implemented a python parser that can decode both structured (specified) and manufacturer specific (non-specified) advertising data. We also provide a user-friendly interface to display the extracted information. Finally, the goal of *Himiko* is to raise users' awareness of privacy issues that the advertising mechanism of BLE devices can imply.

2 THE HIMIKO TOOL

The *Himiko* tool is based on a three-step process. First, advertisement packets emitted by a BLE device are captured through a Bluetooth interface. Then, the raw data are parsed and processed to extract information that can both defeat the randomization mechanism and be used to infer attributes of the owner. Finally, the

[1] https://www.bluetooth.com/specifications/assigned-numbers

results of the processing are displayed as a feedback to the user. The architecture of the tool is presented in Figure 1.

To capture the advertisement packets, our tool only requires two Bluetooth cards supporting the BLE protocol. This is the case for most basic off-the-shelf Bluetooth cards on modern computers running a Unix-like system. Nearby devices are detected using the Received Signal Strength Indication (RSSI) and using external dongles such as a CSR v4.0 Bluetooth USB dongle[2] can simplify the estimation of proximity of users' devices.

The tool is composed of three main files. The first one, `orchestrator.sh`, is a bash script configuring the Bluetooth interfaces to enter in the BLE scanning mode featured by the *bluepy*[3] python library. The latter outputs the captured advertising raw data in a string stream, which can then be parsed and processed in real-time by the second python script, `demo.py`. This script is composed of three python modules – `parserModule`, `profilerModule` and `searchingModule` – that respectively parse the advertising raw data, fetch the internal BLE services database of the device and search for this device on Google Shopping or Qwant marketplaces. Finally, `hmi.html` embeds web technologies (css, javascript and php) that structure and beautify the results of the analysis before to be displayed in a Mozilla Firefox web browser.

The knowledge base used by the `parserModule` to decode advertisement packets has been built from the online official Bluetooth SIG resources, third-party public resources such as the *advlib*[4] advertisement packet decoding library, the *RaMBLE*[5] Android mobile application and the *bleah*[6] BLE scanner tool, but also from the reverse engineering of the *Apple* Handoff, *Microsoft* Connected Devices Platform and *Google* Nearby proximity protocols [2].

The only information captured by our tool are data contained in advertisement packets sent by BLE devices having an enabled Bluetooth interface. Traffic data sent by associated devices, timing or physical-layer information are not considered. The display includes the metadata of the advertisement packet (device addr., type of addr., etc.), a list of the extracted information, an inference of the device type based on its advertised device name along with a dump of the internal BLE services database of the device. Note that, such a database is readable by default as the Bluetooth Core Specification [6, Vol 3, Part G, sec. 8.1] does not consider included information as private or confidential. Finally, when a BLE device broadcasts its device name, the owner of the involved device can decide to provide additional information[7] on the device in order to improve the device identification capabilities of *Himiko*.

To minimize privacy risks for the users of our tool, we apply the minimization principle and keep as little necessary information as possible. In particular, all collected data are kept in memory during the processing time before being immediately erased when the results are displayed to the users. Furthermore, the tool only detects devices in close range of the antenna (a few centimeters) to ensure that only volunteering participants will have their data collected and processed.

3 INTERACTION WITH PARTICIPANTS

During the demonstration, participants will be able to interact with *Himiko* by testing the information broadcasted by their BLE enabled devices. By bringing their device close to the Bluetooth antennas of *Himiko*, they will trigger a capture event that will record an advertisement packet emitted by their device. Such a packet contains raw data that will be parsed then processed by the tool to compute a comprehensive analysis of the emitted information of the device. The results of this process will be displayed as a feedback to the user on a screen. Figure 2 presents an example of the output triggered by a *Chipolo Classic*[8] BLE keyring device. In addition, when a device advertises its device name, participants will have the opportunity to contribute to the knowledge base of *Himiko* by providing additional information on their device.

4 CONCLUSION

We introduced *Himiko*, a user-friendly tool to shed light on the privacy issues of BLE enabled devices. The objective of this tool is to raise awareness on 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. In fact, the specifications do not provide any guidelines about the content of the advertising payload regarding the privacy implications. In addition, we aim to raise public awareness with regard to the information that can be exposed by their BLE enabled devices.

ACKNOWLEDGEMENTS

This work was supported by the SPIE ICS-INSA Lyon IoT chair.

REFERENCES

[1] Bluetooth SIG. 2018. *Bluetooth Market Update 2018.* Technical Report. https://www.bluetooth.com/markets/market-report

[2] Guillaume Celosia and Mathieu Cunche. 2019. Saving Private Addresses: An Analysis of Privacy Issues in the Bluetooth-Low-Energy Advertising Mechanism. Under evaluation.

[3] Aveek K Das, Parth H Pathak, Chen-Nee Chuah, and Prasant Mohapatra. 2016. Uncovering privacy leakage in ble network traffic of wearable fitness trackers. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications*. ACM.

[4] Kassem Fawaz, Kyu-Han Kim, and Kang G Shin. 2016. Protecting Privacy of BLE Device Users.. In *USENIX Security Symposium.*

[5] Dieter Oosterlinck, Dries F Benoit, Philippe Baecke, and Nico Van de Weghe. 2017. Bluetooth tracking of humans in an indoor environment: An application to shopping mall visits.

[6] Bluetooth SIG. 2019. *Bluetooth Core Specification v5.1.* https://www.bluetooth.com/specifications/bluetooth-core-specification

[7] Mathy Vanhoef, Celestin Matte, Mathieu Cunche, Leonardo S. Cardoso, and Frank Piessens. 2016. Why MAC Address Randomization is Not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security (ASIA CCS '16).* ACM.

[8] Ford-Long Wong and Frank Stajano. 2005. Location privacy in bluetooth. In *Security and privacy in ad-hoc and sensor networks.*

[2] https://tinyurl.com/y5kobwf6

[3] https://github.com/IanHarvey/bluepy

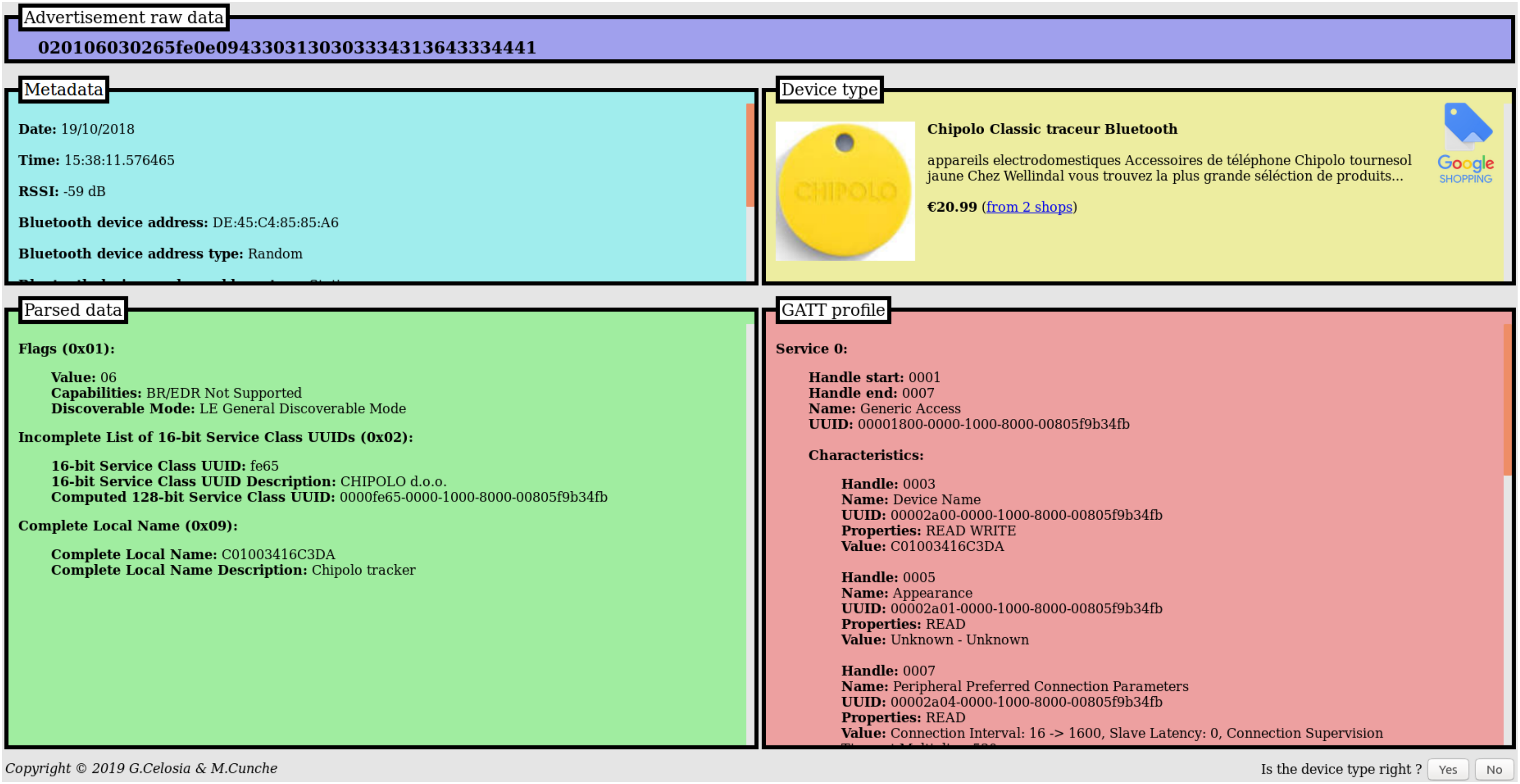
[4] https://github.com/reelyactive/advlib

[5] https://www.contextis.com/en/resources/tools/ramble-ble-app

[6] https://tinyurl.com/yag4cers

[7] Assisted by the operator, the owner can provide a regular expression matching the device name along with information such as the vendor, model and type.

[8] https://chipolo.net/en/products/chipolo-classic



Advertisement raw data

020106030265fe0e0943303130303334313643334441

Metadata

Date: 19/10/2018

Time: 15:38:11.576465

RSSI: -59 dB

Bluetooth device address: DE:45:C4:85:85:A6

Bluetooth device address type: Random

Device type

Chipolo Classic traceur Bluetooth

appareils electrodomestiques Accessoires de téléphone Chipolo tournesol jaune Chez Wellindal vous trouvez la plus grande séléction de produits...

€20.99 (from 2 shops)

Parsed data

Flags (0x01):

- **Value:** 06
- **Capabilities:** BR/EDR Not Supported
- **Discoverable Mode:** LE General Discoverable Mode

Incomplete List of 16-bit Service Class UUIDs (0x02):

- **16-bit Service Class UUID:** fe65
- **16-bit Service Class UUID Description:** CHIPOLO d.o.o.
- **Computed 128-bit Service Class UUID:** 0000fe65-0000-1000-8000-00805f9b34fb

Complete Local Name (0x09):

- **Complete Local Name:** C01003416C3DA
- **Complete Local Name Description:** Chipolo tracker

GATT profile

Service 0:

Handle start: 0001
Handle end: 0007
Name: Generic Access
UUID: 00001800-0000-1000-8000-00805f9b34fb

Characteristics:

Handle: 0003
Name: Device Name
UUID: 00002a00-0000-1000-8000-00805f9b34fb
Properties: READ WRITE
Value: C01003416C3DA

Handle: 0005
Name: Appearance
UUID: 00002a01-0000-1000-8000-00805f9b34fb
Properties: READ
Value: Unknown - Unknown

Handle: 0007
Name: Peripheral Preferred Connection Parameters
UUID: 00002a04-0000-1000-8000-00805f9b34fb
Properties: READ
Value: Connection Interval: 16 -> 1600, Slave Latency: 0, Connection Supervision

Copyright © 2019 G.Celosia & M.Cunche

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