Wombat: An experimental Wi-Fi tracking system

Célestin Matte, Mathieu Cunche

Wombat: An experimental Wi-Fi tracking system

Célestin Matte, Mathieu Cunche
Univ Lyon, INSA Lyon, Inria, CITI, France

Abstract

In this paper, we present Wombat, a Wi-Fi tracking platform aiming at improving user awareness toward physical tracking technologies and at experimenting new privacy-preserving mechanisms. Elements of this system are presented along with its architecture. We also present the use of Wombat in the context of a demonstration scenario. We introduce a new privacy-enhancing feature developed on top of Wombat: a Wi-Fi-based opt-out mechanism that allows users to easily express their opt-out decision.

1 Introduction

Whether it is through websites or mobile applications, user tracking is a common thing in the digital world. This practice of monitoring users' activity for analytics or profiling purposes has recently been extended to the physical world, where radio and video technologies now allow to accurately detect, recognize and categorize human activities [24, 23, 10].

This work focuses on the radio flavor of physical tracking, in which radio signals emitted by our mobile devices are collected in order to infer our activities in the physical world [23]. Radio-based physical tracking relies on sniffers that collect identifiers contained in messages emitted by radio-enabled devices [14]. These identifiers are used to detect users' presence and estimate their mobility. Because Wi-Fi is included in many portable devices and relatively easy to sniff, it is the main radio technology used in the physical tracking industry.

Nowadays, physical tracking systems are deployed in shopping centers [10], urban transportation systems, highways or ring roads [5]. Because these systems passively collect identifiers without user consent (and often without their knowledge), they are the source of major privacy concerns [20, 12]. Despite some efforts from the industry and close surveillance from data protection authorities, users' privacy is still in jeopardy [13, 1, 25]. This is aggravated by the fact that this technology is not well known by the general public, usually not aware that such systems exist and that passers-by may have been tracked.

The goal of this work is to remedy to this situation by raising public awareness towards tracking technologies. To this end, we have developed an experimental Wi-Fi-based physical tracking system that can be used for demonstration purposes. This system effectively tracks users through their radio-enabled mobile devices (e.g. smartphones) and can then show the users the type and amount of data that has been collected. In addition, this experimental platform is also used to deploy and test privacy-enhancing features for physical tracking systems.

After presenting some background and related works in section 2 and 3, we present the experimental physical tracking system in section 4. Then, in section 5, we present how this system is used for raising user awareness. Finally, in section 6, we present an example of privacy-preserving feature. Section 7 concludes the paper.

2 Wi-Fi-based physical tracking

A key element of infrastructure-based Wi-Fi networks is the ability for the stations (devices equipped with a Wi-Fi interface) to discover available networks. This feature called *service discovery* is enabled by two distinct mechanisms. One of them, called the active service discovery mode, relies on probe request messages that are sent by stations and to which access points reply with *probe responses*.

Stations using this mechanism thus periodically and automatically broadcast probe requests. As most Wi-Fi frames, probe requests include the MAC address of the sender, a globally unique identifier tied to a device. Because of its superior energy efficiency, the active discovery mode is enabled on most Wi-Fi devices. As a consequence, all mobile devices having their Wi-Fi interface enabled broadcast a unique identifier and expose their owner to tracking [14].

This kind of tracking is performed by Wi-Fi-based systems that collect messages coming from Wi-Fi-enabled devices in order to detect the people's presence and track their whereabouts. These systems are typically composed of several *sniffing* nodes that are in charge of collecting Wi-Fi signals over an area of interest. Each sniffing node collects incoming Wi-Fi frames and extracts a unique identifier along with other technical information. Nodes then report this data to a central server, where it can be stored and processed for further analysis, such as building trajectories and aggregate statistics.

3 Related Works

Privacy issues in Wi-Fi tracking systems: Because of their passive and pervasive nature, Wi-Fi tracking systems have raised a number of privacy concerns [12, 20, 28]. Stakeholders of the Wi-Fi tracking industry have reacted by adopting a Mobile Location Analytics Code of Conduct [16]. The latter is a set of guidelines, including "anonymization" and opt-out, supposed to reduce privacy risks. However, a number of these measures are ineffective in protecting users' privacy [25, 1, 13].

Data protection authorities have taken actions by fining some Wi-Fi tracking companies [17] or by blocking the deployment of Wi-Fi tracking systems [11]. Parallelwise, the smartphone and computer industry is taking steps to protect users against tracking by deploying MAC randomization mechanisms in their products [31, 18, 3, 29]. However, these countermeasures are not always sufficient to protect against tracking [30, 19].

Experimental Wi-Fi tracking systems: Research and hacking communities have noticed the possibility of tracking users through Wi-Fi signals, which lead to the development of several systems to demonstrate tracking potential.

G. Wilkinson proposed Snoopy, a distributed Wi-Fi tracking system that can include a drone as a sniffing node [32, 2]. CreepyDoll is another Wi-Fi surveillance system that features a distributed data storage [9]. Scheuner et al. introduced Probr [27], a Wi-Fi tracking systems providing extensive analytics features. The *Digital Marauder's Map* [15] is a system that demonstrates the possibility of getting fine-grained users location, using multiple sniffers.

In [26], Robyns et al. built a tracking system using low-cost MikroTik 5RB912UAG-2HPnD devices as nodes.

Panoptiphone [21] is a prototype that demonstrates fingerprinting of Wi-Fi devices based on technical characteristics of frames.

The closest related work is the effort conducted by Bonne et al. They introduced WiFiPi, a tracking system that have been used to monitor mass events such as a music festival [6]. Then, they presented a system called SASQUATCH [7, 8] which aims at raising awareness by displaying information leaked by smartphones, including information that can be inferred from SSIDs. In addition to the demonstration purposes of their work, our approach possesses a strong emphasis on the experimentation of new privacy features.

4 Wombat: a Wi-Fi tracking platform

Wombat is a fully functional Wi-Fi tracking platform supporting three main features: collection, storage/processing, query/output. These three features are implemented through a distributed infrastructure composed of:

- **Sensor nodes**: small devices with wireless monitoring capabilities. They collect information sent on wireless channels and forward it to the server.
- **Central server**: the central entity of the system. It receives data sent by sensor nodes and then stores it in an internal data structure. It is also in charge of answering queries related to the stored data.

To ensure communication between the sensor nodes and the server, the *Wombat* system relies on a wired network (Ethernet). In addition, Wombat can be enriched with a *user interface* and an *opt-out node*:

- **User interface**: a device in charge of displaying detailed information about one or several tracked devices (see Figure 2). The device to display can be specified manually by its MAC address or through proximity detection.
- **Opt-out node**: an element in charge of implementing an opt-out mechanism for users refusing to be tracked by the system (see section 6).

A description of the Wombat system with all its components is presented on Figure 1.

5 Raising user awareness

Users are generally not aware that Wi-Fi tracking is possible and are even less aware that it is actually used by commercial entities. This can be explained by

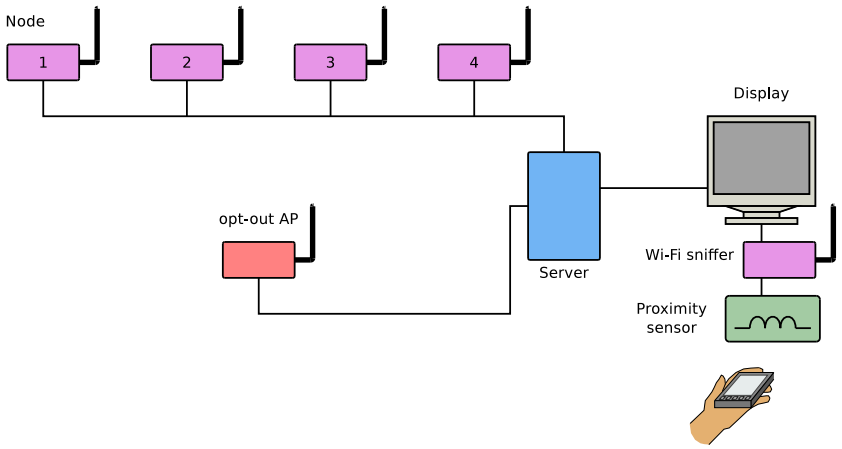

Figure 1: Architecture of the Wombat system in a demonstration configuration.

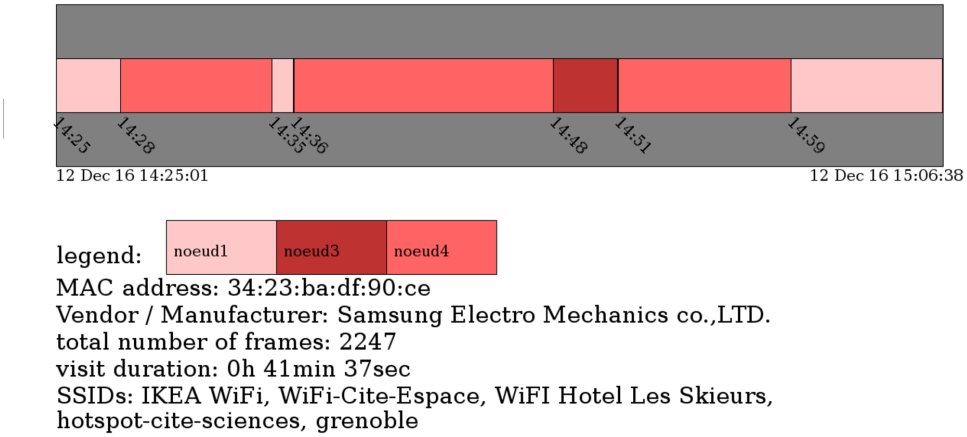

Figure 2: Basic user interface of Wombat displaying the device's MAC address, the list of SSIDs, as well as a mobility trace under a timeline form.

the fact that tracking is performed using radio signals, a technology that leaves no visible traces. Moreover, the visual notifications displayed by trackers are generally obscure.

For the sake of transparency, it is therefore important to show people that such technologies exist, and to explain their principles and their capabilities. Wombat has been developed in this spirit: to raise user awareness by demonstrating a real-world Wi-Fi tracking system.

Although Wombat lacks some of the functionalities found in industrial Wi-Fi tracking systems, it features their core functionalities: device identification and detection, itinerary tracking. These functionalities are enough to present the principles of a Wi-Fi tracking system and to initiate a discussion on the corre-

sponding privacy issues. The Wombat system has been used during demonstrations addressed to different types of audiences: researchers, students, industrials, and general public.

The Wombat system is currently deployed at *La Cité des Sciences et de l'Industrie*, a museum dedicated to science popularization in France. It is part of a one-year-long exhibition (April 2017 - March 2018) on data and digital technologies called *Terra Data*[1]. Wombat is deployed all over the exhibition using 9 sensor nodes, a server node and an opt-out node. It is accompanied by a user interface developed by a third party.

The demonstration scenario is the following. Visitors exploring the exhibition are tracked through Wi-Fi signals emitted by their personal devices. At the entrance, they are notified of the system's presence and of the opt-out mechanism. In the last part of the visit, they reach the user interface where they can explore the information that has been collected on them. Through a proximity sensor combined with a Wi-Fi interface, the system detects the device that is placed on the stand. From there, an interactive screen displays the collected data: identifier, brand of the device, name of the networks searched by the device, and an approximate representation of the user itinerary inside the exhibition.

This last demonstration has the potential to enlighten a large number of individuals from the general public. People aware of the potential privacy issues will be more inclined to adopt solutions to protect their privacy, and to ask for better privacy protections, either legal or technical.

6 Privacy-enhancing feature: Opt-Out Mechanism

6.1 Current opt-out mechanisms and their limitations

Wi-Fi tracking systems have been criticized because they are collecting users' data without their consent. As a result, opt-out mechanisms have been deployed [16] to allow concerned users to escape tracking. These opt-out mechanisms typically involve a webpage on which the user needs to enter its device address[2] (see Figure 3).

Although, it represents a step toward more user control, this kind of approach presents several issues, mainly related to their usability. The main issues are the following:

1. In order to retrieve the MAC address, users need to navigates deep into the device's settings, which can be a difficult task for non-tech-savvy users.

2. Users need to manually enter this 16-character-long identifier on the opt-out webpage, which can be a cumbersome task.

3. Subscribing to the opt-out mechanisms means that the device identifier will be sent to a third party which will store it indefinitely.

[1] `http://www.cite-sciences.fr/fr/vous-etes/enseignants/votre-visite/expositions/terra-data/`

[2] `https://smart-places.org/`

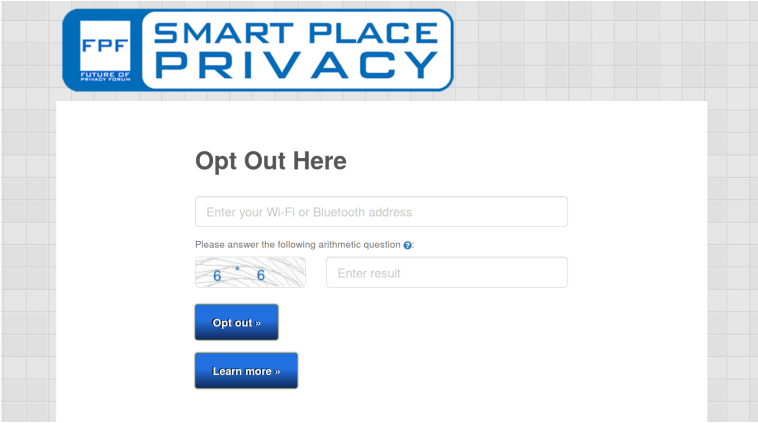

Figure 3: Screenshot of a the opt-out webpage `https://optout.smart-places.org/`. The user needs to enter the address of its device to opt out.

4. Multiple tracking systems may use different opt-out databases and thus require users to go through this process for each system.

It is likely that these usability issues will deter users from using this opt-out mechanisms, thus preventing them from protecting their privacy. A more usable opt-out solution is therefore required.

6.2 A Wi-Fi-based opt-out mechanism

We propose to use Wi-Fi as a vector to transmit the opt-out decision, by leveraging core Wi-Fi elements. More specifically, on the tracking system side, the opt-out mechanism is implemented by a *primitive*[3] Access Point (AP), to which Wi-Fi stations willing to opt out must connect.

The network name (SSID) announced by this AP is explicitly indicating the purpose of the network: opting out of a Wi-Fi tracking system. For instance, this SSID can be `Opt-Out Wi-Fi tracking` or `Do not track`.

A device whose owner wants to opt out will connect to this AP. Upon such an event, the device will contact the AP in order to proceed through the association protocol. During this process, the AP will learn the MAC address of the device by parsing received frames. From this point on, the AP can consider that the corresponding device wants to opt out of the tracking system, and can thus add this address to a local blacklist. This list is maintained locally, and an expiry delay can be configured on the server so that blacklisted identifiers are not kept indefinitely.

For the user, the opt-out procedure can be summarized as follow:

1. Open the Wi-Fi network manager;

[3]This AP is primitive because it does not provide any service other than announcing its presence and allowing devices connections. In particular, it does not provide IP connectivity, i.e. no network connection is possible. Because of this lack of network connectivity, most devices will disconnect automatically after a certain period of time.

2. Identify and select the opt-out network;

3. Connect to the opt-out network.

From a user point of view, this opt-out mechanism involves a small number of simple tasks with which most users are familiar: identifying and connecting to a Wi-Fi network. Thus, we provide a user experience which won't discourage users from actually opting out of the system.

Concerning the device, Wi-Fi-based opt-out is supported by all Wi-Fi devices providing a user interface, which is the case for the majority of devices carried around by people (smartphone, tablets, laptops, ...). In addition it has the big advantage of not requiring any software or hardware modification.

On the Wi-Fi tracking system side, only minor modifications must be performed: a primitive AP must be deployed and must be linked to the Wi-Fi tracking system in order to report opting out MAC addresses.

Another advantage of this method is its persistence and its seamless nature: next time the device will detect an opt-out AP using the same SSID, it will automatically notify its willingness to opt out without requiring any user intervention. Indeed, as the device has already been successfully connected to the opt-out network, the latter is configured and will be remembered by the device's network manager. As a consequence, next time the device will come in range of an AP advertising this opt-out SSID, it will connect to this AP, effectively indicating its intent to opt out.

A global opt-out mechanism for Wi-Fi tracking could be implemented if all stakeholders agree on a common SSID. This mechanism could then be seen as an equivalent of the web-based *Do-Not-Track* (DNT) mechanism [22] for the physical world.

7 Conclusion

We introduced Wombat, an experimental Wi-Fi tracking system. We showed how it can be used as a demonstration tool in order to raise user awareness. Then we showed how this platform can be used as a basis to develop and test privacy-preserving mechanisms. The first one of such mechanisms, a Wi-Fi-based opt-out mechanism, has been presented. It has the advantage of being easy to implement and to use be end users.

We envision to develop the demonstrative aspects of Wombat, by including other radio technologies, improving the trajectory reconstruction algorithm, and extending the user interface. We also plan to integrate other privacy preserving features to Wombat such as privacy-preserving analytics [4].

References

[1] Privacy trade-offs in retail tracking | Federal Trade Commission.

[2] sensepost/Snoopy.

[3] Android 6.0 changes. Retrieved from `https://developer.android.com/about/versions/marshmallow/android-6.0-changes.html`, 2015.

[4] Mohammad Alaggan, Mathieu Cunche, and Marine Minier. Privacy-Preserving t-Incidence for WiFi-based Mobility Analytics. July 2016.

[5] Atec ITS France. *Evaluations simultanées de différentes technologies innovantes de recueil de données trafic pour le calcul de temps de parcours en temps réel*, 2015.

[6] B. Bonné, A. Barzan, P. Quax, and W. Lamotte. WiFiPi: Involuntary tracking of visitors at mass events. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a*, pages 1–6, June 2013.

[7] Bram Bonné, Wim Lamotte, Peter Quax, and Kris Luyten. Raising Awareness on Smartphone Privacy Issues with SASQUATCH, and solving them with PrivacyPolice. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pages 379–381. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2014.

[8] Bram Bonné, Peter Quax, and Wim Lamotte. Your Mobile Phone is a Traitor!–Raising Awareness on Ubiquitous Privacy Issues with SASQUATCH. 2014.

[9] Brendan O'Connor. CreepyDOL: Cheap, Distributed Stalking. Technical report, 2013.

[10] Brian Fung. How stores use your phone's WiFi to track your shopping habits, October 2013.

[11] Claire Bouchenard. JC Decaux's pedestrian tracking system blocked by French data regulator, October 2015.

[12] Stephanie Clifford and Quentin Hardy. Attention, Shoppers: Store Is Tracking Your Cell. *The New York Times*, July 2013.

[13] Levent Demir, Mathieu Cunche, and Cédric Lauradoux. Analysing the privacy policies of Wi-Fi trackers. pages 39–44. ACM Press, 2014.

[14] Julien Freudiger. How talkative is your mobile device?: an experimental study of Wi-Fi probe requests. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, page 8. ACM, 2015.

[15] X. Fu, N. Zhang, A. Pingley, W. Yu, J. Wang, and W. Zhao. The Digital Marauder's Map: A New Threat to Location Privacy. In *2009 29th IEEE International Conference on Distributed Computing Systems*, pages 589–596, June 2009.

[16] Future of Privacy Forum. Mobile Location Analytics Code of Conduct. Technical report, Future of Privacy Forum, October 2013.

[17] Megan Geuss. Creepy but legal phone-tracking company gets wrist slap for empty privacy promise, April 2015.

[18] Emmanuel Grumbach. iwlwifi: mvm: support random MAC address for scanning. Linux commit `effd05ac479b`.

[19] Jeremy Martin, Travis Mayberry, Collin Donahue, Lucas Foppe, Lamont Brown, Chadwick Riggins, Erik C. Rye, and Dane Brown. A Study of MAC Address Randomization in Mobile Devices and When it Fails. *arXiv:1703.02874 [cs]*, March 2017. arXiv: 1703.02874.

[20] Jennifer Martinez. Franken still unsatisfied with Euclid's privacy practices. *TheHill*, April 2013.

[21] Célestin Matte and Mathieu Cunche. DEMO: Panoptiphone: How Unique is Your Wi-Fi Device? In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, WiSec '16, pages 209–211, New York, NY, USA, 2016. ACM.

[22] Jonathan Mayer, Arvind Narayanan, and Sid Stamm. Do Not Track: A Universal Third-Party Web Tracking Opt Out. Internet-Draft draft-mayer-do-not-track-00, Internet Engineering Task Force, March 2011. Work in Progress.

[23] A. B. M. Musa and Jakob Eriksson. Tracking Unmodified Smartphones Using Wi-fi Monitors. In *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems*, SenSys '12, pages 281–294, New York, NY, USA, 2012. ACM.

[24] Le T. Nguyen, Yu Seung Kim, Patrick Tague, and Joy Zhang. IdentityLink: user-device linking through visual and RF-signal cues. pages 529–539. ACM Press, 2014.

[25] Parker Higgins and Lee Tien. Mobile Tracking Code of Conduct Falls Short of Protecting Consumers, October 2013.

[26] Pieter Robyns, Bram Bonné, Peter Quax, and Wim Lamotte. Non-cooperative 802.11 mac layer fingerprinting and tracking of mobile devices. *Security and Communication Networks*, 2017.

[27] J. Scheuner, G. Mazlami, D. Schöni, S. Stephan, A. De Carli, T. Bocek, and B. Stiller. Probr - A Generic and Passive WiFi Tracking System. In *2016 IEEE 41st Conference on Local Computer Networks (LCN)*, pages 495–502, November 2016.

[28] Sen. Al Franken. Sen. Franken Presses Tech Firm to Stop Tracking Consumers without Their Permission | Al Franken | Senator for Minnesota.

[29] Katie Skinner and Jason Novak. Privacy and your app. In *Apple Worldwide Dev. Conf. (WWDC)*, June 2015.

[30] Mathy Vanhoef, Célestin Matte, Mathieu Cunche, Leonardo S. Cardoso, and Frank Piessens. 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, pages 413–424, New York, NY, USA, 2016. ACM.

[31] Winkey Wang. Wireless networking in Windows 10. In *Windows Hardware Engineering Community conference (WinHEC)*, March 2015.

[32] Glenn Wilkinson. Digital terrestrial tracking: The future of surveillance. Technical report, DEFCON, 2014.