Privacy issues in wireless networks: Every frame you send, they'll be watching you.

Mathieu Cunche

N° Identificateur

HABILITATION À DIRIGER DES RECHERCHES

présentée devant

l'Institut National des Sciences Appliquées de Lyon
et l'Université Claude Bernard LYON 1

Privacy issues in wireless networks

Every frame you send, they'll be watching you.

Spécialité : Informatique

par

Mathieu Cunche

Soutenue le 02/06/2021 devant la Commission d'examen

Noubir Guevara	Professeur, Northeastern University	Rapporteur
Fischer-Hübner Simone	Professeure, Karlstad University	Rapporteur
Anciaux Nicolas	Directeur de recherche, Université de Versailles/St-Quentin	Rapporteur (absent)
Guérin Lassous Isabelle	Professeure, Université Claude Bernard Lyon 1	Examinateur
Gorce Jean-Marie	Professeur, INSA-Lyon	Examinateur
Zuniga Juan Carlos	SigFox	Examinateur

CITI Lab - Centre d'Innovation en Télécommunications et Intégration des Services

Remerciements

Ce document et les contributions qui y sont associées ont pu voir le jour grâce aux personnes que j'ai pu croiser à travers mon parcours. Tout d'abord, l'ensemble de l'équipe Inria Privatics et en particulier Vincent Roca et Claude Casteluccia qui ont eu l'étrange idée de respectivement me prendre en thèse et de m'accueillir dans leur équipe. Je dois remercier aussi Cédric Lauradoux et sa connaissance encyclopédique des chroniques de Ganache, Daniel Le Métayer puit de connaissances en matière de lois et règlements en tous genres, Nataliia Bielova et ses idées percutantes, Antoine Boutet et son incroyable dynamisme, et bien évidement Helen et son aide si précieuse.

Ces travaux ont principalement été conduits au sein du laboratoire CITI et je remercie l'ensemble de ses membres avec qui j'ai échangé pour faire émerger des idées ou simplement pour apprendre de nouvelles connaissances. Il me faut également remercier l'ensemble du Network Research Group du NICTA où j'ai entamé ces travaux : Roksana Boreli et Aruna Serevinatne qui m'ont accueilli et Dali avec qui j'ai conduit des travaux passionnants.

Le contenu de ce document est issu des travaux menés avec deux personnes que j'ai eu la chance d'encadrer durant leur thèse : Célestin Matte et Guillaume Celosia. Ils ont l'un comme l'autre fournis un travail exceptionnel et je suis fier d'avoir été leur encadrant.

Avant que je prenne la direction de la recherche, ma trajectoire a été influencée par un nombre d'enseignants qui mon accompagnés à des moments clefs. Je pense en particulier à Samuel Viollin, Thierry Dugardin, et finalement Jean-Louis Roch.

Je souhaite aussi remercier Juan Carlos Zuniga et Amelia Andersdotter sans qui mes contributions à la standardisation n'auraient pas pu voir le jour.

Je tiens à remercier les rapporteurs de ce document, Guevara Noubir, Simone Fischer-Hübner et Nicolas Anciaux ainsi que les autres membres du Jury, Isabelle Guérin Lassous, Jean-Marie Gorce et Juan Carlos Zuniga.

La qualité typographique de ce manuscrit ne serait pas ce qu'elle est sans Lucy Davies que je remercie pour ses relectures.

Finalement, je profite de ce moment pour remercier ma famille pour son soutien et tout particulièrement Sophie, et mes trésors Océane et Eloïse qui illuminent mon quotidien.

Abstract

A growing number of devices carried by users are equipped with wireless technologies such as Bluetooth and Wi-Fi which allow the seamless exchange of information between devices and the network infrastructure. Because they routinely emit wireless messages carrying identifiers and other technical artifacts in cleartext, these technologies expose users to privacy issues. Focusing on the data included in advertising messages, we identify and analyze the leakage of personal data, and study potential and existing countermeasures.

More specifically, we try to answer the following questions: what are the privacy threats associated with wireless networks? Which solutions can be deployed to protect users against these threats? How efficient are current privacy protection implementations?

We start by an analysis of privacy features of the two major wireless network standards: Wi-Fi and Bluetooth-Low-Energy. We focus our study on address randomization mechanisms, a recently adopted anti-tracking measure, and identify several issues related to implementation as well as standard specifications. To illustrate the diversity and complexity of the issues affecting these technologies, we present two representative cases of personal data leakage in wireless networks. First, leveraging the reverse-engineering of *Continuity*, a BLE-based protocol developed by Apple, we uncover a collection of personal data leakages affecting billions of devices worldwide. Finally, we present an abuse of Android Wi-Fi permission that can be used to bypass permissions and to infer personal data such as the location of the device.

When confronted with those privacy issues, it becomes necessary to increase user protection by developing privacy-preserving mechanisms but most importantly by correctly implementing existing ones. Furthermore, it appears that standard specifications are key elements of a better protection, and it is thus of utmost importance to promote the integration of privacy protection in these standards.

Résumé

Un nombre croissant d'équipements intègre une des technologies sans-fil, telles que le Wi-Fi et le Bluetooth, qui permettent des échanges d'informations entre les appareils et le réseau. La transmission de messages incluant des identifiants et des informations techniques en clair expose les utilisateurs de ces technologies à des problèmes de vie privée. En nous concentrant sur les informations exposées par les messages d'*advertising*, nous identifions et analysons la fuite de certaines données personnelles et nous étudions de potentielles contre-mesures. Plus spécifiquement, nous tâchons de répondre aux questions suivantes : quelles sont les menaces sur la vie privée dans les réseaux sans-fil ? Quelles solutions peuvent être mises en place pour protéger les utilisateurs ? Quelle est l'efficacité des protections actuellement déployées ?

Nous commençons par l'analyse des mécanismes de protection de la vie privée dans deux technologies majeures : le Wi-Fi et le Bluetooth-Low-Energy (BLE). Notre étude centrée sur les mécanismes d'adresse aléatoire, une protection anti-traçage récemment adoptée par l'industrie, identifie plusieurs problèmes liés à l'implémentation ainsi qu'aux spécifications des standards.

Afin d'illustrer la diversité et la complexité des problèmes affectant ces technologies, nous présentons deux cas représentatifs de fuite de données personnelles dans les réseaux sans-fil. Premièrement, en nous appuyant sur une rétro-ingénierie de *Continuity*, un protocole d'Apple basé sur le BLE, nous mettons à jour une collection de failles affectant des milliards d'appareils à l'échelle mondiale. Puis, nous présentons un détournement de la permission Wi-Fi d'Android qui permet de contourner les protections du système afin d'obtenir des données personnelles telles que la localisation.

Face à ces problèmes de vie privée, il est nécessaire d'améliorer la protection des utilisateurs en développant des mécanismes de protection et, aussi et surtout, en s'assurant de l'implémentation correcte des mécanismes existants. De plus, il apparait que les spécifications des standards jouent un rôle clef dans la protection de la vie privée ; il est donc de la plus haute importance de promouvoir l'intégration de la protection des données personnelles au sein de ces standards.

Table of contents

Chapter 1

Introduction

1.1 Context

1.1.1 Wireless devices

Last two decades have seen the development of portable electronic devices. It started with laptop computers, then tablets and smartphones, and more recently a flurry of accessories such as smartwatches, wristbands, earphones; today's users can be carrying half a dozen connected objects. A feature shared by these devices is the wireless connectivity which allows them to operate without having to be physically linked to another device or to an infrastructure. A user is thus accompanied by a set of devices that communicate wirelessly to provide them with a variety of utilities (general computing activities, audio/video communications, health monitoring, quantified self, smart-home, etc.).

In portable devices, Bluetooth and Wi-Fi are the two most popular wireless technologies and the aforementioned examples of device use at least one of them. Wi-Fi is a technology mainly used to connect appliances with the network infrastructure, most of the time to provide Internet connectivity. On the other hand, Bluetooth is used to establish connection between two devices belonging to a user, for instance to connect a smartwatch and a smartphone. Although based on two different standards, Wi-Fi and Bluetooth share a number of elements such as the frequency bands on which they operate, the structure of some identifiers, and also the fact that they use packet-based transmissions.

1.1.2 Wireless medium as an attack surface

Wireless communications use radio waves as a medium to carry messages. On this open medium, messages transmitted as radio-frequency signals can be intercepted by any

receiver within range. For this reason, wireless communications are especially vulnerable to attacks, and their securization has been a very active topic for both the academy and the industry. From the release of Wi-Fi and Bluetooth, their security has been heavily tested leading to the development of theoretical and practical advances. One of the main outcomes of these efforts is the release of tools for the capture of wireless signals with off-the-shelf hardware, allowing any tech-savvy user to collect Wi-Fi and Bluetooth signals emitted by nearby devices.

Security research on Wi-Fi and Bluetooth has mainly focused on aspects like confidentiality (breaking encryption mechanisms and retrieving keys) and availability (denial of service and jamming). Until recently, the privacy aspects of these technologies have seldom been discussed and privacy of wireless networks was a relatively unexplored field.

1.1.3 Personal data in (wireless) networks

The development of the Internet and the digital economy is paired with the development of privacy considerations. With the growing usage of computer networks to exchange messages, and to access information and services, personal data has emerged as a central matter in computer networks. Data and metadata resulting from the activity of users on these networks is collected for purposes ranging from commercial profiling to simple surveillance. Nowadays, privacy is considered by a large part of the world as an important matter and recent years have seen the development of technological tools and legal frameworks to protect users (e.g. GDPR and e-Privacy regulation). Many technological efforts have focused on protecting the confidentiality of content (e.g. TLS/SSL) and endpoints (e.g. Tor network) in Internet communications, as well as countering tracking and profiling on the Web.

Little effort has been dedicated to the analysis of the privacy on the edge networks that are Wi-Fi and Bluetooth. These networks are not exempt from prying "antennas" willing to collect personal data available on the airwaves. The 2010's have seen the emergence of *wireless trackers*, entities tracking the physical whereabouts of users thanks to the signals emitted by their portable devices (see Figure 1.1). With the growing number of wireless devices and associated applications, other invasive mechanisms leveraging wireless signals are likely to emerge.

Figure 1.1: *Wi-Fi bins* by Renew were displaying targeted advertisements in the streets of London. Using a Wi-Fi sniffer collecting the identifiers of nearby phones, the system was able to build a profile of pedestrians and to display advertisement messages on a screen mounted on the side of the bin. These bins have been removed following a complaint by the City of London (https://www.bbc.com/news/technology-23665490). Source: Renew.

1.2 Thesis statement

Privacy issues in networks are often seen as the problem of protecting the confidentiality of the data they conveyed. Indeed, the payload of network packets may include elements related to personal data such as text messages, audio, video, visited webpage, etc. In wireless networks such application data is rarely directly exposed because it is protected by one or more layers of encryption (e.g. WPA2-3 and TLS). Nevertheless, even if application data is not exposed, usage of wireless technologies is not exempt from privacy issues.

In this thesis, we show that technical information exposed by personal devices on the wireless link layer can be leveraged to expose personal data. Device identifiers allowing tracking of users are a good example of this technical information, but there are many other cases where diverse items of personal data can be leaked. Information resulting in privacy leakage can be found in wireless messages of any type (data, control, management, etc.). In our work, we focus on traffic that is not directly related to the application layer (i.e. data traffic), but rather to network management traffic such as messages generated by advertising and service discovery mechanisms.

In this thesis, we try to answer the following three questions:

Q1 - What are the existing privacy threats? A first step to ensure personal data protection is to identify the threats and create an inventory of existing and potential issues. Each issue will be characterized by the source of information as well as the nature of the personal data that can be obtained.

Q2 - Which protections to counter these threats? Once identified, comes the question of finding solutions to remove these threats or at least to mitigate them. These solutions may be a simple correction of an implementation mistake, or they can be a more general principle that can be used as guidelines for the design and implementation of wireless systems.

Q3 - How efficient in practice are existing protections? Protection mechanisms started to appear in real-world implementations quickly after the first privacy issues were made public. Thorough evaluation of these implementations is required to confirm that the advertised privacy features are actually protecting users.

Answers to those questions are interleaved throughout the chapters of this thesis.

1.3 Summary of contributions

This section provides a quick overview of the contributions presented in this document. These contributions have been selected based on their scientific significance as well as their impact outside the academic community.

Contributions presented in this thesis are organized in two parts. The first part focuses on an analysis of privacy features in Wi-Fi and Bluetooth, while the second part presents representative examples of how personal data can leak from wireless networks.

1.3.1 Privacy features in wireless networks

The first part of this thesis deals with the physical tracking threat and introduces other privacy threats (Q1) affecting Wi-Fi and Bluetooth. As physical tracking is the main privacy issue for which protection mechanisms are currently widely deployed, we focus on those implementations, and we evaluate their efficiency (Q3). Finally, on the strength of our observations, we are able to devise a number of recommendations to improve user protection (Q2) in particular with regard to the physical tracking threat.

In Chapter 2, we focus on the early implementations of address randomization in Wi-Fi. We demonstrate that those implementations, mainly developed by Apple and Android without a formal specification, were affected by a number of flaws. First, we identified that the content of Wi-Fi packets is diverse enough to create a fingerprint that can be leveraged for tracking. Then we showed that an artifact of the physical layer can be used to link consecutive random addresses. Finally, we presented a number of active attacks that can fully defeat address randomization by forcing the device to reveal its real address.

Chapter 3 presents an analysis of privacy in Bluetooth-Low-Energy. Based on a large-scale measurement campaign, we found that address randomization was activated in a significant fraction of BLE devices, but that a number of devices did not correctly follow the specification of the standard. We found a number of flaws that can defeat address randomization: static identifiers and synchronization issues in the address rotation process. We discovered technical artifacts that can be used for tracking but also to infer technical information on the device such as vendor, model, type, version etc.

1.3.2 Three representative cases of personal data leaks

The second part of this thesis is mainly dedicated to the discovery of new privacy threats (Q1). Focusing on advertising mechanisms of Wi-Fi and Bluetooth, we present two cases illustrating the leakage of personal data through wireless networks. These discoveries call for a number of short-term corrections of wireless systems but also indicates the need for a profound revision of standards and their implementation (Q2). We found that protection mechanisms are scarce and when they are implemented, they often fall short at preventing leakage of personal data (Q3).

Chapter 4 is dedicated to the analysis of a family of BLE-based protocols used by Apple devices. Based on a reverse-engineering of those protocols, called Continuity, we identified a collection of flaws affecting all Apple devices. These flaws expose users to tracking, and leakage of personal information such as user activity on the device and in a smart-home, email and phone numbers, as well as personal assistant voice commands.

In Chapter 5, we consider privacy attacks that can be performed by a mobile application having access to Wi-Fi functionalities. Focusing on the Android system, we show that an application with the `ACCESS_WIFI_STATE` can infer a broad range of personal data. In particular, we show that this permission can be leveraged to obtain the location of the user without its consent or knowledge. We discovered that this flaw was already exploited by third party libraries and was used to illegitimately collect the location of users.

1.3.3 Other contributions not included in this manuscript

This section presents a brief overview of contributions that are not presented in detail in this manuscript but are related to the general problematic of this thesis.

Practical approaches for wireless tracking Focusing on Wi-Fi tracking we discussed several techniques to track an individual [56]. We also considered an hypothetical

botnet composed of wireless routers and evaluated the potential for large scale tracking [124].

Timing based attacks We considered attacks that leverage the timing of wireless frames to infer information on the device. First we used the timing of Wi-Fi probe-requests to derive a fingerprint and thus defeat address randomization [111]. Then we studied how the state of the device can be inferred from the timing variation of Bluetooth "pings" [42].

Inference from SSIDs We investigated the privacy threat that represents SSIDs (Wi-Fi network names) exposed by and in mobile devices, and showed that they can reveal social links between users [59] and also that they can be associated with locations and venues [126].

GATT profile fingerprinting Bluetooth devices expose a GATT profile that includes a range of technical information. We found that many devices publicly expose these profiles and that the corresponding information can threaten the owner's privacy, in particular by allowing the building of a fingerprint that can be used for tracking [43].

Wireless features on mobile operating systems As disabling wireless interfaces is often presented as a way to evade wireless tracking, we investigated [112] whether this was the case and found that a smartphone may still emit Wi-Fi frames even if it has been disabled. We also discovered that the Android system has flaws that allows the bypassing of restrictions on Bluetooth scanning [138].

Privacy in wireless tracking systems In [66] we analyzed the privacy practices of Wi-Fi tracking companies and identified several issues; in particular, we showed the inefficiency of hash function for the anonymization of MAC addresses [67]. We proposed a scheme to implement analytics features in Wi-Fi tracking systems (e.g. counting visitors) while providing strong privacy guarantees [14].

Consent and information in the IoT Wireless signals are not only a source of issue but can also be leveraged to implement privacy features. We proposed a system that uses Bluetooth to implement an information and consent framework for the IoT systems [41].

Ultrasound based tracking Tracking mobile devices is not limited to wireless signals and can be performed through ultrasounds. In [57], we analyzed a real-world system that leveraged ultrasonic beacons to track users via applications with the microphone permission.

1.4 Impact of this research

The work presented in this thesis had an impact outside the academic community and this section lists its main outcomes.

1.4.1 Fixes in Google Android

In response to issues identified in our research, several modifications were made to the Android mobile system. The first example is regarding the issues of Wi-Fi address randomization. Android 8 (2017) included several changes to device identifiers for which we were credited[1]. These changes focused on the problem we discussed in Chapter 2, namely in Wi-Fi probe requests, "the initial packet sequence number for each scan is randomized" and "Unnecessary Probe Request Information Elements have been removed".

The second example, is about the `ACCESS_WIFI_STATE` permission (see Chapter 5). Shortly after the publication of our paper in 2014, the first version of Android 6 (2015) included new restrictions[2] to thwart the attack described in our paper: access to Wi-Fi scan results now requires the location permission. As opposed to the first modification, Android did not credit our work as a motivation for this change.

We have recently been in contact with Google regarding the BLE related issues in Chapter 3 and we hope that this will lead to improvements in future implementation.

1.4.2 Regulation enforcement: FTC vs InMobi

The results of our research on the `ACCESS_WIFI_STATE` permission (see Chapter 5) initiated a case by the US Federal Trade Commission (2015) that resulted in a fine of $950.000 for InMobi, a mobile marketing company. When the case settlement was published, we were informed by the FTC that our paper "WifiLeaks: Underestimated Privacy Implications of the `ACCESS_WIFI_STATE` Android Permission" [13] triggered

[1] https://android-developers.googleblog.com/2017/04/changes-to-device-identifiers-in.html

[2] https://developer.android.com/about/versions/marshmallow/android-6.0-changes.html#behavior-hardware-id

an investigation by the FTC. The agency extended[3] our work and found that InMobi was tracking millions of users without their consent, ignoring their privacy preferences, and in some cases violating the Children's Online Privacy Protection Act (COPPA)[4].

1.4.3 The IEEE 802(.11) working group

Following our first research on Wi-Fi, I got involved in privacy efforts conducted within several working groups at IEEE 802 (the standardization body behind Wi-Fi specifications). Since 2014, my involvement consisted in sharing the most recent advances of the research comunity and contributing to some documents of the working groups[5]. In particular, I am one of the contributors to the recently published standard *802E-2020 Recommended Practice for Privacy Considerations for IEEE 802 Technologies* [144], which includes recommendations covering most of the issues discussed in Chapter 2, and for which I received an *IEEE SA Working Group Chair Awards*[6] for "outstanding contributions".

1.4.4 Dissemination: Data Protection Authorities

We took actions to share the outcome of our research to groups who might be able to act upon them, namely data protection authorities and legislators. Our results were shared on one occasion with members of the French legislative body[7] and more regularly with the CNIL through its Digital Innovation Lab[8][9].

A key item of those contributions was my talk in 2017 on *Cyber-Physical Tracking* at the 62nd meeting of the *Working Group on Data Protection in Telecommunications*

[3] A deep dive into mobile app location privacy following the InMobi settlement https://www.ftc.gov/news-events/blogs/techftc/2016/08/deep-dive-mobile-app-location-privacy-following-inmobi-settlement

[4] Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked

[5] List of my contributions at IEEE 802 https://mentor.ieee.org/privecsg/documents?is_dcn=cunche

[6] https://standards.ieee.org/about/awards/wgchair/index.html

[7] Digital event at the French Senate - 2015 www.senat.fr/evenement/journee_numerique_inria.html

[8] CNIL's lab blog post on Privacy in standards https://linc.cnil.fr/fr/juan-carlos-zuniga-and-mathieu-cunche-privacy-issues-are-still-not-systematically-considered-all

[9] CNIL's lab blog post on deactivation of Wi-Fi on Android https://linc.cnil.fr/fr/desactiver-le-wi-fi-android-ne-nous-preserve-pas-du-tracage

(IWGDPT)[10], a group composed of representatives of the Data Protection Authorities of dozens of countries worldwide as well as NGOs.

1.4.5 Vulgarization: Terra Data exhibition

Part of our efforts were dedicated to science popularization actions that aimed at sharing the results of our research with the people potentially threatened by the privacy issues we have discovered. On this topic, a major achievement was the inclusion of our Wi-Fi tracking demonstrator in the *Terra Data* exhibition that took place at *Cité des Sciences et de l'Industrie* in Paris from 2017 to 2018. Through this exhibition, located in the biggest science museum in Europe, the Wi-Fi tracking issue was presented to approximately 156.000 visitors. A follow-up of this event was our participation in the *Fête de la Science* that took place at the same location in 2017 and during which our demonstration was broadcast on *Sciences & Vie TV*[11].

1.5 Content & structure of the document

The first part of this document presents a privacy analysis of Wi-Fi (Chapter 2) and Bluetooth-Low-Energy (Chapter 3) with a focus on address randomization . The second part presents two cases of personal data leaks associated with wireless networks: first the presentation of privacy leaks affecting the BLE-based Apple Continuity protocols (Chapter 4), then how the Wi-Fi permission on Android can be abused to infer various personal data (Chapter 5).

Verbatim content of published papers In this document each chapter (with the exception of Chapters 1 and 6) presents a contribution associated with a single publication. I have selected the contributions that I consider as having the highest scientific significance and impact. Some contributions have their section of lesser importance removed; aside this, only marginal modifications have been made to the original papers. Therefore, the content of each chapter is almost identical to that of the associated papers. As these papers are addressing similar topics, some redundancy might appear between the background sections of some chapters.

The publications corresponding to each chapter are presented below and indicated at the beginning of each chapter:

[10] https://www.datenschutz-berlin.de/
[11] https://youtu.be/iou1cTzoC0I?t=6141

- Chapter 2: 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. ISBN 978-1-4503-4233-9. doi: 10.1145/2897845.2897883. URL http://doi.acm.org/10.1145/2897845.2897883. event-place: Xi'an, China

- Chapter 3: Guillaume Celosia and Mathieu Cunche. Saving Private Addresses: An Analysis of Privacy Issues in the Bluetooth-Low-Energy Advertising Mechanism. In *MobiQuitous 2019 - 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pages 1–10, Houston, United States, December 2019. doi: 10.1145/3360774.3360777. URL https://hal.inria.fr/hal-02394629

- Chapter 4: Guillaume Celosia and Mathieu Cunche. Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols. *Proceedings on Privacy Enhancing Technologies*, 2020(1):26–46, January 2020. ISSN 2299-0984. doi: 10.2478/popets-2020-0003. URL https://content.sciendo.com/view/journals/popets/2020/1/article-p26.xml

- Chapter 5: Jagdish Prasad Achara, Mathieu Cunche, Vincent Roca, and Aurélien Francillon. Short Paper: WifiLeaks: Underestimated Privacy Implications of the Access_wifi_state Android Permission. In *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks*, WiSec '14, pages 231–236, New York, NY, USA, 2014. ACM. ISBN 978-1-4503-2972-9. doi: 10.1145/2627393.2627399. URL http://doi.acm.org/10.1145/2627393.2627399. event-place: Oxford, United Kingdom

Part I

Privacy Provisions in Wireless Networks

Chapter 2

Defeating MAC address randomization in Wi-Fi

Abstract:

We present several novel techniques to track (unassociated) mobile devices by abusing features of the Wi-Fi standard. This shows that using random MAC addresses, on its own, does not guarantee privacy.

First, we show that information elements in probe requests can be used to fingerprint devices. We then combine these fingerprints with incremental sequence numbers, to create a tracking algorithm that does not rely on unique identifiers such as MAC addresses. Based on real-world datasets, we demonstrate that our algorithm can correctly track as much as 50% of devices for at least 20 minutes. We also show that commodity Wi-Fi devices use predictable scrambler seeds. These can be used to improve the performance of our tracking algorithm. Finally, we present two attacks that reveal the real MAC address of a device, even if MAC address randomization is used. In the first one, we create fake hotspots to induce clients to connect using their real MAC address. The second technique relies on the new 802.11u standard, commonly referred to as Hotspot 2.0, where we show that Linux and Windows send Access Network Query Protocol (ANQP) requests using their real MAC address.

Associated paper: 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. ISBN 978-1-4503-4233-9. doi: 10.1145/2897845.2897883. URL http://doi.acm.org/10.1145/2897845.2897883. event-place: Xi'an, China

Chapter 3

An Analysis of Privacy Provisions in the BLE Advertising Mechanism

Abstract:

The Bluetooth Low Energy (BLE) protocol is being included in a growing number of connected objects such as fitness trackers and headphones. 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 address with random temporary pseudonyms, called Private addresses.

In this chapter, we analyze the privacy issues associated with the advertising mechanism of BLE, leveraging a large dataset of advertisement packets collected in the wild. First, we identified that some implementations fail at following the BLE specifications on the maximum lifetime and the uniform distribution of random identifiers. Furthermore, we found that the payload of the advertisement packet can hamper the randomization mechanism by exposing counters and static identifiers. In particular, we discovered that advertising data of Apple *and* Microsoft *proximity protocols can be used to defeat the address randomization scheme. Finally, we discuss how some elements of advertising data can be leveraged to identify the type of device, exposing the owner to inventory attacks.*

Associated paper: Guillaume Celosia and Mathieu Cunche. Saving Private Addresses: An Analysis of Privacy Issues in the Bluetooth-Low-Energy Advertising Mechanism. In *MobiQuitous 2019 - 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pages 1–10, Houston, United States, December 2019. doi: 10.1145/3360774.3360777. URL https://hal.inria.fr/hal-02394629

Part II

Two representative cases of personal data leaks

Chapter 4

Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols

Abstract:

Apple Continuity protocols are the underlying network component of Apple Continuity *services which allow seamless nearby applications such as activity and file transfer, device pairing and sharing a network connection. Those protocols rely on Bluetooth Low Energy (BLE) to exchange information between devices: Apple Continuity messages are embedded in the payload of BLE advertisement packets that are periodically broadcasted by devices. Recently, Martin et al. identified [109] a number of privacy issues associated with Apple Continuity protocols; we show that this was just the tip of the iceberg and that Apple Continuity protocols leak a wide range of personal information.*

In this work, we present a thorough reverse engineering of Apple Continuity protocols that we use to uncover a collection of privacy leaks. We introduce new artifacts, including identifiers, counters and battery levels, that can be used for passive tracking, and describe a novel active tracking attack based on Handoff messages. Beyond tracking issues, we shed light on severe privacy flaws. First, in addition to the trivial exposure of device characteristics and status, we found that HomeKit accessories betray human activities in a smarthome. Then, we demonstrate that AirDrop and Nearby Action protocols can be leveraged by passive observers to recover

e-mail addresses and phone numbers of users. Finally, we exploit passive observations on the advertising traffic to infer Siri voice commands of a user.

Associated paper: Guillaume Celosia and Mathieu Cunche. Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols. *Proceedings on Privacy Enhancing Technologies*, 2020(1):26–46, January 2020. ISSN 2299-0984. doi: 10.2478/popets-2020-0003. URL https://content.sciendo.com/view/journals/popets/2020/1/article-p26.xml

Chapter 5

Abusing Android's ACCESS_WIFI_STATE Permission to Infer Personal Data

Abstract:

On Android, users can choose to install an application, or not, based on the permissions it requests. These permissions are later enforced on the application by the system, e.g., when accessing sensitive user data. In this work, we focus on the access to Wi-Fi related information, which is protected by the `ACCESS_WIFI_STATE` *permission. We show that this apparently innocuous network related permission can leak Personally Identifiable Information (PII). Such information is otherwise only accessible by clearly identifiable permissions (such as* `READ_PHONE_STATE` *or* `ACCESS_FINE_LOCATION` *or* `ACCESS_COARSE_LOCATION`*). We analyzed permissions of 2700 applications from Google Play, and found that 41% of them use the* `ACCESS_WIFI_STATE` *permission. We then statically analyzed 998 such applications and, based on the results, selected 88 for dynamic analysis. Finally, we conducted an online survey to study the user perception of the privacy risks associated with this permission. Our results demonstrate that users largely underestimate the privacy implications of this permission, in particular because they often cannot realize what private information can be inferred from it. Our analysis further reveals that some companies have already started to abuse this permission to collect personal user information, for example, to get a unique device*

identifier for tracking across applications or to geolocalize the user without explicitly asking for the dedicated permissions. Because this permission is very common, most users are potentially at risk. There is therefore an urgent need for modification of the privileges granted by this permission as well as a more accurate description of the implications of accepting a permission.

Associated paper: Jagdish Prasad Achara, Mathieu Cunche, Vincent Roca, and Aurélien Francillon. Short Paper: WifiLeaks: Underestimated Privacy Implications of the Access_wifi_state Android Permission. In *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks*, WiSec '14, pages 231–236, New York, NY, USA, 2014. ACM. ISBN 978-1-4503-2972-9. doi: 10.1145/2627393.2627399. URL http://doi.acm.org/10.1145/2627393.2627399. event-place: Oxford, United Kingdom

Part III

Conclusion

Chapter 6

Conclusions & Perspectives

6.1 Conclusions

This document presented a collection of contributions showing the main privacy challenges in modern wireless networks. This section presents elements to answer the three questions raised in the introduction (Section 1.2).

6.1.1 Q1 - Identification of privacy threats

We showed that a wide range of privacy issues exist, diverse from the point of view of the data on which they are based, but also on the personal information they can expose. Threats originate from the exposure of metadata (e.g. identifiers and counters found in headers and unencrypted frame bodies) exposed in wireless messages and sometimes from poorly protected data (e.g. lack of encryption of some Apple Continuity payloads).

6.1.1.1 Physical tracking

As illustrated in the introduction, physical tracking is one of the most serious threats for users of wireless devices. We showed that this problem is not constricted to the device address but is also linked to many elements of the wireless signals. We presented a collection of practical approaches to track a device over time without having to rely on the address of the device.

6.1.1.2 Leakage of personal information

Wireless signals generated and collected by wireless interfaces can be leveraged to infer personal data. Our results show that it is not enough to protect carried data traffic

with encryption, as headers and payload of advertising frames can be a trove of personal information.

Furthermore, the use of discovery traffic to carry data for connection-less application such as the *proximity protocols* of Apple, Microsoft and Google is associated with many privacy issues. This practice is allowed by the standards (*manufacturer specific* and *vendor specific* fields of Wi-Fi and Bluetooth) but their implementation is sometime done without serious consideration for privacy protection, resulting in the exposure of several items of personal data.

6.1.1.3 Threats from outside and inside

The majority of threats presented in this document are associated with an external attacker that is monitoring wireless signals emitted by the device of the victim. However, we also saw in Chapter 5 that the attacker can be located inside the device of the victim (e.g. an application) where they leverages wireless functionalities of the device to infer information (e.g. location). When considering the threat associated with a wireless technology, it is therefore necessary to consider what is wirelessly broadcast by the device, but also what can be wirelessly sensed by the device. The latter is particularly important in devices that can run semi-trusted applications potentially harvesting personal data. This inside threat is still very valid, as illustrated by the recent discovery [64] of an app with 10M+ installations that was found to collect and report identifiers of nearby Bluetooth devices, although its functionalities have nothing to do with Bluetooth (it is a bubble level application).

6.1.1.4 Creativity and boldness of trackers

Another lesson learned during this last decade of research on wireless networks is about the creativity and boldness of tracking companies. Several of the attacks considered in our research were first purely hypothetical, and were later found to be exploited by some companies to surreptitiously collect personal data. This is for instance the case of Euclid, a company that started working on Wi-Fi tracking as early as 2011[1] at the same time we were analyzing how this data could threaten privacy [59]. Similarly, on the abuse of the Wi-Fi permission of Android (Chapter 5), it is only after having developed a proof-of-concept that we realized that this weakness was already exploited by major actors of the mobile tracking industry.

[1] https://techcrunch.com/2011/11/03/euclid-elements-emerges-from-stealth-debuts-google-analytics-for-the-real-world/

It appears that there will always be entities ready to collect and exploit personal data by any technical means, even if it is unlawful. It is thus necessary to consider all possible attack scenarios, even those that first seem circumvoluted. This research may prove to be an early warning sign upon which vendors and data protection authorities can act.

6.1.2 Q2 - Solutions

In the course of our research the discovery of new privacy threats was often followed by discussions on potential solutions. In many cases, simply applying the minimization principle to reduce the amount of exposed metadata is enough to thwart the privacy threat (e.g. removing some Information Elements from probe requests). When "sensitive" pieces of data have to be transmitted, encryption or obfuscation schemes must be employed to protect it.

6.1.2.1 Recommendations for address randomization

Address randomization is a key solution to counter the tracking threats. However, as shown in this manuscript it suffers many pitfalls and its use must be complemented with additional rules to ensure its efficiency. Based on our research, we provide a set of recommendations on address randomization as an anti-tracking measure:

- [NO-ID] No identifiers should be included in frames unless strictly necessary.
- [OBFUSCATION] Elements included in frames (identifiers, technical data) should be encrypted or obfuscated whenever possible.
- [DATA-MINIMIZATION] The information embedded in frames should be minimized to reduce the fingerprinting potential. In particular, technical information such as version numbers, supported features, etc. should only be included when strictly needed.
- [ROTATION] Identifiers, counters and other stateful fields must be reset to a random value whenever the address rotates.
  - [ROTATION-CPRNG] Random values must be generated using a cryptographic PRNG.
  - [ROTATION-SYNCHRO] A strict synchronization must be enforced between the rotation of the address and the other fields.

  - [ROTATION-RANDOM-TIMING] Randomness should be introduced in the timing of address rotation to prevent tracking attacks leveraging timing.

- [RANDOM-TRANSMIT-TIMING] Randomness should be introduced in the timing of frame transmission to prevent fingerprinting based on timing.

This list is not exhaustive and should be enriched as new threats are discovered. As of now, a strict application of these guidelines should protect against most known attacks.

6.1.2.2 Evolution of standards specification

When considering privacy protection in the context of wireless networks, standards and technical specifications appear to play a significant role. Beyond the application of guidelines like the ones presented above, it is necessary to include privacy considerations in the development of standards.

Our research shows that the standards themselves are to blame for some privacy issues affecting wireless networks. One source of these problems is the lack of privacy provisions in the wireless standards of Wi-Fi (IEEE 802.11) and Bluetooth. Entire sections of those standards are dedicated to security mechanisms, but the protection of personal data is rarely considered[2]. Privacy mechanisms are often entwined with other elements of the specifications, it is thus important to apply a privacy by design approach in which protection mechanisms are fully integrated in the development process.

Furthermore, we have observed that even when privacy specifications are included in the standard, vendors often fail to implement them correctly, thus releasing products with botched privacy protections. This suggests a poor integration of privacy requirements in the product development process, but also a lack of verification during the product certification phase.

Standards must thus evolve to include more privacy considerations and in parallel, a correct implementation of the privacy-preserving features must be more strictly enforced.

6.1.2.3 Better control of wireless functionalities

We saw that the access to wireless functionalities by mobile applications can lead to serious privacy issues. It is therefore necessary to consider the wireless interfaces as a fully-fledged sensor and apply the same restriction that would be applied to any other sensor on a mobile device (e.g. a camera or a GPS module). Mobile operating systems

[2]We note that this situation is currently evolving positively with the introduction of address randomization for both Bluetooth and IEEE 802.11.

have initiated efforts in this direction by implementing permission-based restriction on some features associated with Wi-Fi and Bluetooth interfaces[3]. Despite these new measures, wireless features are still abused by some applications [64]. Further restrictions may be required to fully protect users. For instance restricting applications to use filtered scans[4] that will report only devices matching a specific criterion (UUID, device name or address prefix, etc.) instead of reporting all visible devices.

6.1.3 Q3 - Efficiency of implemented protections

Issues exist within the implementation of privacy preserving mechanisms, some of them serious enough to totally negate the protection. In this document, we focused on the main privacy protection included in wireless devices: address randomization.

6.1.3.1 Implementation issues with Address Randomization

More than 5 years after its first use in mainstream devices, address randomization is still affected by issues. A number of these implementation issues are coming from mistakes or overlooked pitfalls, which can be easily fixed once identified (e.g. non-reset counters). Others are more fundamental and will require considerable advances or modification of the protocols to be fixed.

We presented in section 6.1.2.1 recommendations for effective address randomization. Among the issues addressed by those recommendations, we have identified two that are recurrent and appear to be challenging to solve in practice: synchronization and fingerprintability.

Synchronization A number of issues in address randomization come from the lack of synchronization between the address rotation process and the content of the frame which can undermine the anti-tracking protection [5]. As mentioned in our recommendations (Section 6.1.2.1), the address change must be done together with a coherent management of the frame content (reset of counter, rotation of identifiers, etc.) and those rotations must be done synchronously.

[3] On Android, the location permission is required for any application using Bluetooth and Wi-Fi scans, and location services must be activated to initiate those scans and obtain the results https://developer.android.com/guide/topics/connectivity/bluetooth https://developer.android.com/guide/topics/connectivity/wifi-scan

[4] Android BLE ScanFilter https://developer.android.com/reference/android/bluetooth/le/ScanFilter

[5] As seen in chapter 2 and 3.

Although those requirements are is easily stated, they have proven rather difficult to implement in practice. Several implementations appear to include such requirements[6], however this rotation is not always fully synchronized: some frames using the old content use the new address (see Figure 6.1) thus undermining the purpose of address randomization.

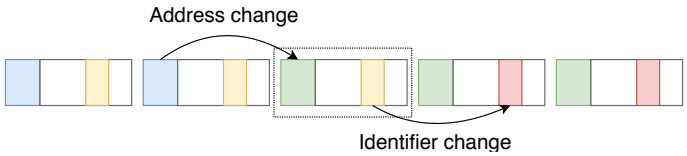

Figure 6.1: Mis-synchronized rotation of address and content in a sequence of frames.

This problem has recently been highlighted [140] in contact tracing applications based on Google-Apple Exposure Notification (GAEN) framework, where the rotations of the BLE device address and the GAEN temporary pseudonym is sometimes not synchronized. This shows the difficulty of this synchronization: Apple and Google are controlling the full BLE stack and the OS, and yet they are not able to fully synchronize the rotations.

The difficulty of synchronizing these rotations comes from a lack of coordination between the MAC layer (which controls the address) and the above layer (the application controlling the content of the frame). Signalization mechanisms between these layers are required to implement a fully synchronized rotation.

Fingerprintability Another element undermining address randomization comes from the quantity and diversity of data included in frames, which can be used to fingerprint devices. New features are regularly added to wireless standards and a growing number of applications are piggybacking on advertisement mechanisms to carry data. As a result, advertisement frames are populated with an increasing number of fields, whose value and order can vary from one device to the other. The fingerprint created with this data can be unique enough to single-out devices and thus allow tracking despite the use of a random address.

This issue is similar to web-browser fingerprinting [69], that has been developed to track users after more persistent identifiers were denied. To the best of our knowledge, wireless fingerprinting is not yet used by wireless trackers. But it is possible that some of them will follow the same path as web trackers by adopting fingerprinting to continue user tracking despite the adoption of address randomization.

[6] In several Apple implementations, the content of the frame is rotating with the same frequency as the address

Finally, fingerprintability goes beyond privacy and might also affect security by allowing attackers to identify the specific model and software version of a device.

6.2 Perspectives

6.2.1 The physical layer

Most of the results presented in this thesis are based on information gathered at the link-layer. However, privacy issues can emerge from the physical layer. For instance, fingerprinting leveraging physical features of the transceiver [61] can be used to single-out and thus track devices. Other physical layer artifacts have already been exploited in this direction: the scrambler seed (as seen in Chapter 2), or the carrier frequency offset [141]. With the development of new features at the physical layer, additional artifacts will be available to mount novel privacy attacks.

A challenge for the implementation of these attacks is the access to physical layer information, which is not possible with off-the-shelf hardware. Therefore, many works [141, 33, 139] relied on *software-define radio* setups to gather this data. Another solution has recently emerged with the reverse-engineering and customization of firmware of off-the-shelf transceivers, as recently demonstrated with BLE [106, 51]. This approach could be applied to other wireless technologies, including Wi-Fi, to facilitate the analysis of privacy issues, and more generally security, at the physical layer.

6.2.2 Automatization of the privacy issues detection

The privacy leaks presented in this document are the results of manual investigations, involving a thorough analysis of traffic traces and code. These tasks are time-consuming, prone to mistakes and non-exhaustive. With the increasing number of implementations and versions of wireless protocols, manual investigation will not scale; a automation of this process is required.

A first step is the verification of implementation against known issues. We have made a first proposal using trace-based verification [47], but verification of properties could also be done on the code using for instance formal methods. The code may not be available, in which case, one would have to rely on black-box verification techniques.

The most challenging task will be to identify unknown issues and especially on protocols whose specifications are not public (for instance Apple Continuity protocols). One possible direction is to use machine learning to identify problematic patterns in

wireless traffic, potentially supported by reverse-engineering techniques to identify packet structures in undocumented protocols.

Furthermore, the verification of privacy features could be integrated in a privacy-oriented certification process. Emerging privacy labels[7] could be generalized or extended to cover wireless devices.

6.2.3 Development and integration of privacy features

Regarding the privacy threats recently discovered around wireless technologies, it appears necessary to develop privacy features that could be integrated in protocol specifications. This task is urgent given the latency of the standard development process.

A first avenue is an improvement of existing privacy mechanisms like address randomization. In particular, as discussed before, the synchronization of the various layers called for the development of cross-layer mechanisms that would ensure that rotation of identifiers is done coherently across all the layers.

Another aspect that could be investigated is the de-correlation of the link layer identifier from other aspects of the network management. In 802.11 networks, the MAC address is used by several mechanisms (security protocols, access control, filtering, monitoring) which make its rotation impractical in a connected scenario. Introducing a new identifier dedicated to those purposes and using the MAC address only for link-layer operations, would facilitate the rotation of the latter.

More generally, privacy-enhancing mechanisms tailored for wireless protocols should be further developed to satisfy the growing requirements of emerging features while protecting users against tracking and leakage of personal data. Advertising mechanisms should receive specific attention as they are currently the main source of the issues. Resolvable identifiers, like BLE *random resolvable addresses* (see section **??**), are a good example of what can be done in this direction.

[7] https://developer.apple.com/news/?id=3wann9gh

Support & collaborations

The contributions presented in this document are the product of research that took place over the last decade (2010-2020) and have been conducted in several scientific environments.

My research on wireless networks started in 2010 when I was a post-doctoral researcher at the *Network Research Group* of NICTA, Australia. I then briefly went back to Inria as a post-doctoral resarcher in 2012. Since 2012, I am an assistant-professor[8] at INSA-Lyon (University of Lyon) as well as a faculty member of the Inria *Privatics* team[9].

Funding and supporting projects

My research on wireless networks and privacy have been supported by several grants and projects listed below in chronological order:

- NICTA's Trusted Networking project;
- Rhône-Alpes region's ARC7 framework: Célestin Matte's PhD scholarship;
- CISCO cyber-grant CG#593780: Mohammad Alaggan's Postdoc;
- The ADAGE project funded by France's Programme d'Investissement d'Avenir[10];
- The INSA/SPIE-ICS IoT chair[11]: Guillaume Celosia's PhD scholarship;
- The Privamov project of University of Lyon[12];

Collaborations

The work presented in this document, and more generally all my research on wireless networks, would not have seen the light without the help of collaborators. First and

[8] Maître de conférences.
[9] https://team.inria.fr/privatics/
[10] P128356-2659748
[11] http://www.citi-lab.fr/chairs/iot-chair/
[12] https://projet.liris.cnrs.fr/privamov/project/

foremost the PhD students that I have supervised, Célestin Matte and Guillaume Celosia; and then by chronological order:

- NICTA/CISRO Data 61: Roksanna Boreli, Mohammed "Dali" Kaafar, Suranga Seneviratne, Fangzhou Jiang, Aruna Seneviratne;
- KU Leuven: Mathy Vanhoef, Frank Piesen;
- INSA-Lyon - CITI: Leonardo Cardoso, Patrice Raveneau;
- Grenoble University - LIG: Frank Rousseau;
- Inria Privatics: Vincent Roca, Jagdish Achara, Cédric Lauradoux, Levent Démir, Amrit Kumar, Pierre Rouveyrol, Mohammad Alaggan;
- Eurecom: Aurélien Francillon
- CNIL/ARCEP: Vincent Toubiana

References

[1] This recycling bin is following you. Quartz.com. 8 août 2013. http://qz.com/112873/this-recycling-bin-is-following-you/.

[2] Android System Permissions Categories. http://developer.android.com/guide/topics/manifest/permission-element.html, .

[3] Android System Permissions Groups. http://developer.android.com/reference/android/Manifest.permission_group.html, .

[4] Tails - privacy for anyone anywhere. Retrieved from https://tails.boum.org.

[5] Androguard. https://code.google.com/p/androguard/, .

[6] The Google Maps Geolocation API. https://developers.google.com/maps/documentation/business/geolocation/, .

[7] Google Play unofficial API. https://github.com/egirault/googleplay-api, .

[8] WiFiManager Class. http://developer.android.com/reference/android/net/wifi/WifiManager.html, .

[9] WiGLE: Wireless Geographic Logging Engine. http://wigle.net/, 2001. URL http://wigle.net/.

[10] Ieee standard for local and metropolitan area networks: Overview and architecture. *IEEE Std 802-2014 (Revision to IEEE Std 802-2001)*, pages 1–74, June 2014. doi: 10.1109/IEEESTD.2014.6847097.

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

[12] Osama Abukmail. Wifi Mac Changer. Retrieved from https://play.google.com/store/apps/details?id=com.wireless.macchanger.

[13] Jagdish Prasad Achara, Mathieu Cunche, Vincent Roca, and Aurélien Francillon. Short Paper: WifiLeaks: Underestimated Privacy Implications of the Access_wifi_-state Android Permission. In *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks*, WiSec '14, pages 231–236, New York, NY, USA, 2014. ACM. ISBN 978-1-4503-2972-9. doi: 10.1145/2627393.2627399. URL http://doi.acm.org/10.1145/2627393.2627399. event-place: Oxford, United Kingdom.

[14] Mohammad Alaggan, Mathieu Cunche, and Sébastien Gambs. Privacy-preserving Wi-Fi Analytics. *Proceedings on Privacy Enhancing Technologies*, 2018(2):4–26, April 2018. doi: 10.1515/popets-2018-0010. URL https://content.sciendo.com/view/journals/popets/2018/2/article-p4.xml. This is a journal:.

[15] Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen. Nearby threats: Reversing, analyzing, and attacking google's' nearby connections' on android. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, February 2019.

[16] Gopala Krishna Anumanchipalli, Kishore Prahallad, and Alan W Black. Festvox: Tools for creation and analyses of large speech corpora. In *Workshop on Very Large Scale Phonetics Research, UPenn, Philadelphia*, page 70, 2011.

[17] Apple. Home accessories. the list keeps getting smarter. . URL https://www.apple.com/ios/home/accessories/. Accessed: 2019-05-25.

[18] Apple. Mfi program. . URL https://developer.apple.com/programs/mfi/. Accessed: 2019-05-25.

[19] Apple. All your devices. one seamless experience. . URL https://www.apple.com/macos/continuity/. Accessed: 2019-05-25.

[20] Apple. Handoff. . URL https://developer.apple.com/handoff/. Accessed: 2019-05-25.

[21] Apple. Apple reports record first quarter results. 2016. URL https://www.apple.com/newsroom/2016/01/26Apple-Reports-Record-First-Quarter-Results/. Accessed: 2019-05-25.

[22] Apple. Connect and use your airpods. 2019. URL https://support.apple.com/en-us/HT207010. Accessed: 2019-05-25.

[23] Apple. About airprint. 2019. URL https://support.apple.com/en-us/HT201311. Accessed: 2019-05-25.

[24] Apple. Use handoff to continue a task on your other devices. 2019. URL https://support.apple.com/en-us/HT209455. Accessed: 2019-05-25.

[25] Apple. *HomeKit Accessory Protocol Specification (Non-Commercial Version) - Release R2*. 2019. URL https://developer.apple.com//homekit/specification/. Accessed: 2019-08-20.

[26] Apple. Use instant hotspot to connect to your personal hotspot without entering a password. 2019. URL https://support.apple.com/en-us/HT209459. Accessed: 2019-08-20.

[27] Apple. *iOS Security - iOS 12.3*. 2019. URL https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf. Accessed: 2019-05-25.

[28] Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick Feamster. Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic. 2017.

[29] Chrisil Arackaparambil, Sergey Bratus, Anna Shubina, and David Kotz. On the reliability of wireless fingerprinting using clock skews. In *Proceedings of the third ACM conference on Wireless network security*, pages 169–174. ACM, 2010.

[30] Marco V. Barbera, Alessandro Epasto, Alessandro Mei, Sokol Kosta, Vasile C. Perta, and Julinda Stefa. CRAWDAD dataset sapienza/probe-requests (v. 2013-09-10). Retrieved 10 November, 2015, from, http://crawdad.org/sapienza/probe-requests/20130910, September 2013.

[31] Johannes K Becker, David Li, and David Starobinski. Tracking anonymized bluetooth devices. *Proceedings on Privacy Enhancing Technologies*, 2019(3):50–65, 2019.

[32] Marianne Bertrand and Emir Kamenica. Coming apart? cultural distances in the united states over time. Technical report, National Bureau of Economic Research, 2018.

[33] B. Bloessl, C. Sommer, F. Dressler, and D. Eckhoff. The scrambler attack: A robust physical layer attack on location privacy in vehicular networks. In *ICNC*, 2015.

[34] Bastian Bloessl, Michele Segata, Christoph Sommer, and Falko Dressler. An IEEE 802.11 a/g/p OFDM receiver for GNU radio. In *SRIF Workshop*, 2013.

[35] Jeffrey R Blum, Daniel G Greencorn, and Jeremy R Cooperstock. Smartphone sensor reliability for augmented reality applications. In *Mobile and Ubiquitous Systems: Computing, Networking, and Services*, pages 127–138. Springer, 2013.

[36] B. Bonne, 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. doi: 10.1109/WoWMoM.2013.6583443.

[37] Joseph Bonneau. The science of guessing: Analyzing an anonymized corpus of 70 million passwords. In *2012 IEEE Symposium on Security and Privacy*, pages 538–552. IEEE, 2012.

[38] Theodore Book, Adam Pridgen, and Dan S Wallach. Longitudinal analysis of android ad library permissions. *arXiv preprint arXiv:1303.0857*, 2013.

[39] Vladimir Brik, Suman Banerjee, Marco Gruteser, and Sangho Oh. Wireless device identification with radiometric signatures. In *MobiCom*, 2008.

[40] Piers O'Hanlon Carlos J. Bernardos, Juan Carlos Zúñiga. Wi-Fi internet connectivity and privacy: hiding your tracks on the wireless internet. In *IEEE CSCN*, 2015.

[41] C. Castelluccia, M. Cunche, D. Le Metayer, and V. Morel. Enhancing Transparency and Consent in the IoT. In *International Workshop on Privacy Engineering, IWPE 2018*, pages 116–119, April 2018. doi: 10.1109/EuroSPW.2018.00023.

[42] Guillaume Celosia and Mathieu Cunche. Detecting smartphone state changes through a bluetooth based timing attack. In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pages 154–159. ACM, 2018.

[43] Guillaume Celosia and Mathieu Cunche. Fingerprinting Bluetooth-Low-Energy Devices Based on the Generic Attribute Profile. In *Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things*, IoT S&P'19, pages 24–31, London, UK, 2019. ACM. ISBN 978-1-4503-6838-4. doi: 10.1145/3338507.3358617. URL https://doi.org/10.1145/3338507.3358617.

[44] Guillaume Celosia and Mathieu Cunche. Saving Private Addresses: An Analysis of Privacy Issues in the Bluetooth-Low-Energy Advertising Mechanism. In *MobiQuitous 2019 - 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pages 1–10, Houston, United States, December 2019. doi: 10.1145/3360774.3360777. URL https://hal.inria.fr/hal-02394629.

[45] Guillaume Celosia and Mathieu Cunche. Saving private addresses: An analysis of privacy issues in the bluetooth-low-energy advertising mechanism. In *Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*. ACM, 2019.

[46] Guillaume Celosia and Mathieu Cunche. Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols. *Proceedings on Privacy Enhancing Technologies*, 2020(1):26–46, January 2020. ISSN 2299-0984. doi: 10.2478/popets-2020-0003. URL https://content.sciendo.com/view/journals/popets/2020/1/article-p26.xml.

[47] Guillaume Celosia and Mathieu Cunche. Valkyrie: A Generic Framework for Verifying Privacy Provisions in Wireless Networks. page 7, 2020.

[48] Chainfire. Pry-Fi. Retrieved from https://play.google.com/store/apps/details?id=eu.chainfire.pryfi.

[49] Indra Mohan Chakravarti, Radha Govira Laha, and Jogabrata Roy. Handbook of methods of applied statistics. *Wiley Series in Probability and Mathematical Statistics (USA) eng*, 1967.

[50] Yu-Chung Cheng, Yatin Chawathe, Anthony LaMarca, and John Krumm. Accuracy characterization for metropolitan-scale wi-fi localization. In *Proceedings of the 3rd International Conference on Mobile Systems, Applications, and Services*, MobiSys '05, pages 233–245, New York, NY, USA, 2005. ACM. ISBN 1-931971-31-5. doi: 10.1145/1067170.1067195. URL http://doi.acm.org/10.1145/1067170.1067195.

[51] Jiska Classen and Matthias Hollick. Inside job: Diagnosing bluetooth lower layers using off-the-shelf devices. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, pages 186–191, 2019.

[52] Bogdan Copos, Karl Levitt, Matt Bishop, and Jeff Rowe. Is anybody home? inferring activity from smart home network traffic. In *2016 IEEE Security and Privacy Workshops (SPW)*, pages 245–251. IEEE, 2016.

[53] Jim Cowie and Wendy Lehnert. Information extraction. *Communications of the ACM*, 39(1):80–91, 1996.

[54] Marius Cristea and Bogdan Groza. Fingerprinting smartphones remotely via ICMP timestamps. *Communications Letters, IEEE*, 17(6):1081–1083, 2013.

[55] Ang Cui, Michael Costello, and Salvatore Stolfo. When firmware modifications attack: A case study of embedded exploitation. 2013.

[56] Mathieu Cunche. I know your MAC address: targeted tracking of individual using Wi-Fi. *Journal of Computer Virology and Hacking Techniques*, 10(4):219–227, November 2014. ISSN 2263-8733. doi: 10.1007/s11416-013-0196-1. URL https://doi.org/10.1007/s11416-013-0196-1.

[57] Mathieu Cunche and Leonardo Sampaio Cardoso. Analyzing Ultrasound-based Physical Tracking Systems. In *GreHack 2018*, Grenoble, France, November 2018. URL https://hal.inria.fr/hal-01927513.

[58] Mathieu Cunche, Mohamed-Ali Kaafar, and Roksana Boreli. Linking wireless devices using information contained in wi-fi probe requests. *Pervasive and Mobile Computing*, 11:56–69, 2014. ISSN 1574-1192. doi: https://doi.org/10.1016/j.pmcj.2013.04.001. URL https://www.sciencedirect.com/science/article/pii/S1574119213000618.

[59] Mathieu Cunche, Mohamed-Ali Kaafar, and Roksana Boreli. Linking wireless devices using information contained in Wi-Fi probe requests. *Pervasive and Mobile Computing*, 11:56–69, April 2014. ISSN 1574-1192. doi: 10.1016/j.pmcj.2013.04.001. URL http://www.sciencedirect.com/science/article/pii/S1574119213000618.

[60] Dino A Dai Zovi, Shane Macaulay, et al. Attacking automatic wireless network selection. In *Proc. of the Sixth Annual SMC Inf. Assurance Workshop*, 2005.

[61] Boris Danev, Davide Zanetti, and Srdjan Capkun. On physical-layer identification of wireless devices. *ACM Computing Surveys (CSUR)*, 45(1):6, 2012.

[62] Cuthbert Daniel and Wilkinson Glenn. Snoopy: Distributed tracking and profiling framework. In *44Con 2012*, 2012.

[63] Aveek K Das, Parth H Pathak, Chen-Nee Chuah, and Prasant Mohapatra. Uncovering privacy leakage in ble network traffic of wearable fitness trackers. In

Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications, pages 99–104. ACM, 2016.

[64] Paul-Olivier Dehaye and Joel Reardon. Swisscovid: a critical analysis of risk assessment by swiss authorities, 2020.

[65] Levent Demir, Mathieu Cunche, and Cédric Lauradoux. Analysing the privacy policies of Wi-Fi trackers. In *Proc. of the 2014 workshop on physical analytics*, 2014.

[66] Levent Demir, Mathieu Cunche, and Cédric Lauradoux. Analysing the Privacy Policies of Wi-Fi Trackers. In *Proceedings of the 2014 Workshop on Physical Analytics*, WPA '14, pages 39–44, New York, NY, USA, 2014. ACM. ISBN 978-1-4503-2825-8. doi: 10.1145/2611264.2611266. URL http://doi.acm.org/10.1145/2611264.2611266. event-place: Bretton Woods, New Hampshire, USA.

[67] Levent Demir, Amrit Kumar, Mathieu Cunche, and Cedric Lauradoux. The Pitfalls of Hashing for Privacy. *IEEE Communications Surveys Tutorials*, 20(1):551–565, 2018. ISSN 1553-877X. doi: 10.1109/COMST.2017.2747598.

[68] Loh Chin Choong Desmond, Cho Chia Yuan, Tan Chung Pheng, and Ri Seng Lee. Identifying unique devices through wireless fingerprinting. In *WiSec*, 2008.

[69] Peter Eckersley. How unique is your web browser? In *Privacy Enhancing Technologies*, 2010.

[70] Kassem Fawaz, Kyu-Han Kim, and Kang G Shin. Protecting privacy of BLE device users. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 1205–1221, 2016.

[71] Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, and David Wagner. Android permissions demystified. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, pages 627–638, New York, NY, USA, 2011. ACM. ISBN 978-1-4503-0948-6. doi: 10.1145/2046707.2046779. URL http://doi.acm.org/10.1145/2046707.2046779.

[72] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 3:1–3:14, New York, NY, USA, 2012. ACM. ISBN 978-1-4503-1532-6. doi: 10.1145/2335356.2335360. URL http://doi.acm.org/10.1145/2335356.2335360.

[73] Jason Franklin, Damon McCoy, Parisa Tabriz, Vicentiu Neagoe, Jamie V Randwyk, and Douglas Sicker. Passive data link layer 802.11 wireless device driver fingerprinting. In *USENIX Security*, 2006.

[74] Julien Freudiger. How talkative is your mobile device? An experimental study of Wi-Fi probe requests. In *WiSec*, 2015.

[75] Hao Fu, Aston Zhang, and Xing Xie. Effective social graph deanonymization based on graph structure and descriptive information. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 6(4):49, 2015.

[76] Nina Gerber, Benjamin Reinheimer, and Melanie Volkamer. Investigating people's privacy risk perception. *Proceedings on Privacy Enhancing Technologies*, 2019(3): 267–288, 2019.

[77] Michelle X Gong, Brian Hart, Liangfu Xia, and Roy Want. Channel bounding and MAC protection mechanisms for 802.11ac. In *GLOBECOM*, 2011.

[78] F. Gont. A method for generating semantically opaque interface identifiers with ipv6 stateless address autoconfiguration (slaac). RFC 7217, 2014.

[79] Google. Nearby. URL https://developers.google.com/nearby/. Accessed: 2019-05-25.

[80] Ben Greenstein, Ramakrishna Gummadi, Jeffrey Pang, Mike Y. Chen, Tadayoshi Kohno, Srinivasan Seshan, and David Wetherall. Can Ferris Bueller still have his day off? protecting privacy in the wireless era. In *Proceedings of the 11th USENIX workshop on Hot topics in operating systems*, pages 10:1–10:6, Berkeley, CA, USA, 2007. USENIX Association. URL http://dl.acm.org/citation.cfm?id=1361397.1361407.

[81] Ben Greenstein, Ramakrishna Gummadi, Jeffrey Pang, Mike Y Chen, Tadayoshi Kohno, Srinivasan Seshan, and David Wetherall. Can ferris bueller still have his day off? protecting privacy in the wireless era. In *HotOS*, 2007.

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

[83] Marco Gruteser and Dirk Grunwald. Enhancing location privacy in wireless LAN through disposable interface identifiers: A quantitative analysis. *Mobile Networks and Applications*, 10(3):315–325, 2005.

[84] Marco Gruteser and Dirk Grunwald. Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis. *Mobile Networks and Applications*, 10(3):315–325, 2005.

[85] Fanglu Guo and Tzi-cker Chiueh. Sequence number-based MAC address spoof detection. In *RAID*, 2006.

[86] Jaap Haitsma and Ton Kalker. A highly robust audio fingerprinting system. In *Ismir*, volume 2002, pages 107–115, 2002.

[87] Christian Huitema. Personal communication, November 2015.

[88] Christian Huitema. Experience with MAC address randomization in Windows 10. In *93th Internet Engineering Task Force Meeting (IETF)*, July 2015.

[89] Mathias Humbert, Mohammad Hossein Manshaei, Julien Freudiger, and Jean-Pierre Hubaux. Tracking games in mobile networks. In *Conf. on Decision and Game Theory for Security*, 2010.

[90] Troy Hunt. The 773 million record "collection #1" data breach. 2019. URL https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/. Accessed: 2019-05-25.

[91] Nathaniel Husted and Steven Myers. Mobile location tracking in metro areas: Malnets and others. In *CCS*, 2010.

[92] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. IEEE Std 802.11-2012, 2012.

[93] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 9: Interworking with External Networks*. IEEE Std 802.11u, 2011.

[94] Taher Issoufaly and Pierre Ugo Tournoux. Bleb: Bluetooth low energy botnet for large scale individual tracking. In *2017 1st International Conference on Next Generation Computing Applications (NextComp)*, pages 115–120. IEEE, 2017.

[95] Mohamed Imran Jameel and Jeffrey Dungen. Low-power wireless advertising software library for distributed m2m and contextual iot. In *Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on*, pages 597–602. IEEE, 2015.

[96] Suman Jana and Sneha Kumar Kasera. On fast and accurate detection of unauthorized wireless access points using clock skews. In *MobiCom*, 2008.

[97] Dorene Kewley, Russ Fink, John Lowry, and Mike Dean. Dynamic approaches to thwart adversary intelligence gathering. In *Proceedings DARPA Information Survivability Conference and Exposition II. DISCEX'01*, volume 1, pages 176–185. IEEE, 2001.

[98] TW Kirkman. Statistics to use: Kolmogorov-smirnov test. *College of Saint Benedict and Saint John's University. Retrieved October*, 7:2008, 1996.

[99] Heiko Knospe. Privacy-enhanced perceptual hashing of audio data. In *2013 International Conference on Security and Cryptography (SECRYPT)*, pages 1–6. IEEE, 2013.

[100] Anthony LaMarca, Yatin Chawathe, Sunny Consolvo, Jeffrey Hightower, Ian Smith, James Scott, Timothy Sohn, James Howard, Jeff Hughes, Fred Potter, et al. Place lab: Device positioning using radio beacons in the wild. In *Pervasive computing*, pages 116–133. Springer, 2005.

[101] P. Leach, M. Mealling, and R. Salz. A universally unique identifier (UUID) URN namespace. RFC 4122 (Proposed Standard), July 2005. URL http://www.ietf.org/rfc/rfc4122.txt.

[102] Scott Lester. The emergence of bluetooth low energy. 2015. URL https://www.contextis.com/blog/the-emergence-of-bluetooth-low-energy. Accessed: 2019-08-30.

[103] Scott Lester and Paul Stone. Bluetooth le - increasingly popular, but still not very private. 2016. URL https://www.contextis.com/en/blog/bluetooth-le-increasingly-popular-still-not-very-private. Accessed: 2019-08-30.

[104] Janne Lindqvist, Tuomas Aura, George Danezis, Teemu Koponen, Annu Myllyniemi, Jussi Mäki, and Michael Roe. Privacy-preserving 802.11 access-point discovery. In *WiSec*, 2009.

[105] Xiaohua Liu, Shaodian Zhang, Furu Wei, and Ming Zhou. Recognizing named entities in tweets. In *Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies-Volume 1*, pages 359–367. Association for Computational Linguistics, 2011.

[106] Dennis Mantz, Jiska Classen, Matthias Schulz, and Matthias Hollick. InternalBlue - Bluetooth Binary Patching and Experimentation Framework. In *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services*, pages 79–90, Seoul Republic of Korea, June 2019. ACM. ISBN 978-1-4503-6661-8. doi: 10.1145/3307334.3326089. URL https://dl.acm.org/doi/10.1145/3307334.3326089.

[107] Jeremy Martin, Erik Rye, and Robert Beverly. Decomposition of mac address structure for granular device inference. In *Proceedings of the 32nd Annual Conference on Computer Security Applications*, pages 78–88. ACM, 2016.

[108] 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. *Proceedings on Privacy Enhancing Technologies*, 2017(4):268–286, 2017.

[109] Jeremy Martin, Douglas Alpuche, Kristina Bodeman, Lamont Brown, Ellis Fenske, Lucas Foppe, Travis Mayberry, Erik Rye, Brandon Sipes, and Sam Teplov. Handoff all your privacy – a review of apple's bluetooth low energy continuity protocol. *Proceedings on Privacy Enhancing Technologies*, 2019(4):34–53, 2019.

[110] Matthias Marx, Ephraim Zimmer, Tobias Mueller, Maximilian Blochberger, and Hannes Federrath. Hashing of personally identifiable information is not sufficient. *SICHERHEIT 2018*, 2018.

[111] Célestin Matte, Mathieu Cunche, Franck Rousseau, and Mathy Vanhoef. Defeating MAC Address Randomization Through Timing Attacks. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, WiSec '16, pages 15–20, New York, NY, USA, 2016. ACM. ISBN 978-1-4503-4270-4. doi: 10.1145/2939918.2939930. URL http://doi.acm.org/10.1145/2939918.2939930. Short paper, 28%.

[112] Célestin Matte, Mathieu Cunche, and Vincent Toubiana. Does disabling Wi-Fi prevent my smartphone from sending Wi-Fi frames? report, Inria - Research Centre Grenoble – Rhône-Alpes ; INSA Lyon, August 2017. URL https://hal.inria.fr/hal-01575519.

[113] Microsoft. *Microsoft Connected Devices Platform Protocol Version 3*. 2019. URL https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-cdp/f5a15c56-ac3a-48f9-8c51-07b2eadbe9b4. Accessed: 2019-05-25.

[114] Bhupinder Misra. iOS 8 MAC randomization – analyzed! http://blog.airtightnetworks.com/ios8-mac-randomization-analyzed/. URL http://blog.airtightnetworks.com/ios8-mac-randomization-analyzed/.

[115] 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. ISBN 978-1-4503-1169-4. doi: 10.1145/2426656.2426685. URL http://doi.acm.org/10.1145/2426656.2426685.

[116] A. B. M. Musa and Jakob Eriksson. Tracking unmodified smartphones using Wi-Fi monitors. In *SenSys*, 2012.

[117] Le T Nguyen, Yu Seung Kim, Patrick Tague, and Joy Zhang. Identitylink: User-device linking through visual and rf-signal cues. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 529–539. ACM, 2014.

[118] Lukasz Olejnik, Gunes Acar, Claude Castelluccia, and Claudia Diaz. The leaking battery. In *Data Privacy Management, and Security Assurance*, pages 254–263. Springer, 2015.

[119] Dieter Oosterlinck, Dries F Benoit, Philippe Baecke, and Nico Van de Weghe. Bluetooth tracking of humans in an indoor environment: An application to shopping mall visits. *Applied geography*, 78:55–65, 2017.

[120] Brendan O'Connor. CreepyDOL: Cheap, distributed stalking. In *BlackHat*, 2013.

[121] Jeffrey Pang, Ben Greenstein, Ramakrishna Gummadi, Srinivasan Seshan, and David Wetherall. 802.11 user fingerprinting. In *MobiCom*, 2007.

[122] Jeffrey Pang, Ben Greenstein, Srinivasan Seshan, and David Wetherall. Tryst: The case for confidential service discovery. In *HotNets*, 2007.

[123] Jeffrey Pang, Ben Greenstein, Srinivasan Seshan, and David Wetherall. Tryst: The Case for Confidential Service Discovery. In *HotNets*, volume 2, page 1, 2007.

[124] Pierre Rouveyrol, Patrice Raveneau, and Mathieu Cunche. Large Scale Wi-Fi tracking using a Botnet of Wireless Routers. page 7, June 2015.

[125] Matthias C Sala, Kurt Partridge, Linda Jacobson, et al. An exploration into activity-informed physical advertising using pest. In *International Conference on Pervasive Computing*, pages 73–90. Springer, 2007.

[126] S. Seneviratne, F. Jiang, M. Cunche, and A. Seneviratne. SSIDs in the wild: Extracting semantic information from WiFi SSIDs. In *2015 IEEE 40th Conference on Local Computer Networks (LCN)*, pages 494–497, October 2015. doi: 10.1109/LCN.2015.7366361.

[127] Sandra Siby, Rajib Ranjan Maiti, and Nils Tippenhauer. Iotscanner: Detecting and classifying privacy threats in iot neighborhoods. *arXiv preprint arXiv:1701.05007*, 2017.

[128] Bluetooth SIG. *Bluetooth Core Specification v4.0*. 2010. URL https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=456433. Accessed: 2019-05-25.

[129] Bluetooth SIG. *Bluetooth Core Specification v5.1*. 2019. URL https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=457080. Accessed: 2019-05-25.

[130] Bluetooth SIG. *Bluetooth Core Specification Supplement v8.0*. 2019. URL https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=457081. Accessed: 2019-08-30.

[131] Bluetooth SIG. Bluetooth market update 2019. Technical report, 2019. URL https://www.bluetooth.com/wp-content/uploads/2018/04/2019-Bluetooth-Market-Update.pdf. Accessed: 2019-08-30.

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

[133] Sparhandy. Siri commands - endless functions of your virtual assistant. URL https://www.sparhandy.de/apple/info/siri-commands/. Accessed: 2019-05-25.

[134] Jon Gunnar Sponas. Things you should know about bluetooth range. 2018. URL https://blog.nordicsemi.com/getconnected/things-you-should-know-about-bluetooth-range. Accessed: 2019-08-20.

[135] Tim Stöber, Mario Frank, Jens Schmitt, and Ivan Martinovic. Who do you sync you are?: smartphone fingerprinting via application behaviour. In *WiSec*, 2013.

[136] Milan Stute, Sashank Narain, Alex Mariotto, Alexander Heinrich, David Kreitschmann, Guevara Noubir, and Matthias Hollick. A Billion Open Interfaces for Eve and Mallory: MitM, DoS, and Tracking Attacks on iOS and macOS Through Apple Wireless Direct Link. page 18, 2019.

[137] Humphrey Taylor. Most people are 'privacy pragmatists' who, while concerned about privacy, will sometimes trade it off for other benefits. *The Harris Poll*, 17 (19):44, 2003.

[138] Vincent Toubiana and Mathieu Cunche. Should Contact-Tracing apps really require to enable GPS? – Unsearcher. URL https://unsearcher.org/should-contact-tracing-apps-really-require-to-enable-gps.

[139] 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. ISBN 978-1-4503-4233-9. doi: 10.1145/2897845.2897883. URL http://doi.acm.org/10.1145/2897845.2897883. event-place: Xi'an, China.

[140] Serge Vaudenay and Martin Vuagnoux. Little Thumb Attack on SwissCovid, September 2020. URL https://vimeo.com/453948863.

[141] Tien Dang Vo-Huu, Triet Dang Vo-Huu, and Guevara Noubir. Fingerprinting wi-fi devices using software defined radios. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pages 3–14, 2016.

[142] Luqing Wang and Chmtha Tellambura. An overview of peak-to-average power ratio reduction techniques for OFDM systems. In *IEEE ISSPIT*, 2006.

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

[144] IEEE 802.1 WG. IEEE 802E-2020 - IEEE Approved Draft Recommended Practice for Privacy Considerations for IEEE 802 Technologies. Technical report, September 2020. URL https://standards.ieee.org/standard/802E-2020.html.

[145] *Hotspot 2.0 (Release 2) Technical Specification v1.1.0*. Wi-Fi Alliance, 2010.

[146] Wi-Fi Alliance. *Wi-Fi Simple Configuration Protocol and Usability Best Practices for the Wi-Fi Protected Setup Program, v2.0.1*, April 2011.

[147] Ford-Long Wong and Frank Stajano. Location privacy in bluetooth. In Refik Molva, Gene Tsudik, and Dirk Westhoff, editors, *Security and Privacy in Ad-hoc and Sensor Networks*, pages 176–188, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg. ISBN 978-3-540-31615-2.

[148] Martin Woolley. Bluetooth technology protecting your privacy. 2015. URL https://www.bluetooth.com/blog/bluetooth-technology-protecting-your-privacy/. Accessed: 2019-05-25.

[149] Xiaoyong Zhou, Soteris Demetriou, Dongjing He, Muhammad Naveed, Xiaorui Pan, XiaoFeng Wang, Carl A. Gunter, and Klara Nahrstedt. Identity, location, disease and more: Inferring your secrets from android public resources. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, pages 1017–1028, New York, NY, USA, 2013. ACM. ISBN 978-1-4503-2477-9. doi: 10.1145/2508859.2516661. URL http://doi.acm.org/10.1145/2508859.2516661.

[150] Asaf Zomet and Shlomo Reuben Urbach. Privacy-aware personalized content for the smart home, September 8 2016. US Patent App. 14/638,937.