

Chapter 68

Identification of Wireless Devices From Their Physical Layer Radio-Frequency Fingerprints

Gianmarco Baldini

European Commission – Joint Research Centre, Italy

Gary Steri

European Commission – Joint Research Centre, Italy

Raimondo Giuliani

European Commission – Joint Research Centre, Italy

ABSTRACT

Extensive research has been performed in recent years for the identification of wireless devices from their radio frequency (RF) emissions. The main idea of identifying a wireless device through its RF emissions is that the electronic circuits and the RF components have specific characteristics determined by the production and manufacturing processes. These characteristics, which result in unique differences, can be used to distinguish a wireless device from another because they appear as subtle modification of the RF signal in space even if the wireless device generates a signal conformant to the standard. This chapter describes the main techniques for the fingerprinting of wireless devices using their RF transmission. There are still some key challenges to overcome. This chapter tries to identify them in this context as well as providing possible approaches to solve them. Further research work is needed to investigate the portability issues between fingerprints taken using different receivers, as well as to identify and remove potential other sources of bias.

INTRODUCTION

Extensive research has been performed in recent years for the identification of wireless devices from their radio frequency (RF) emissions both intentional or unintentional. The term “intentional” is used to identify the RF emissions generated by a wireless device to implement a specific wireless standard. For

DOI: 10.4018/978-1-5225-7598-6.ch068

example, the RF emission of the uplink transmission of a mobile phone, which implements a specific wireless communication standard. The term “unintentional” instead, identifies the RF emissions not directly related to the services offered by the wireless device or the wireless standard, but which are generated due to the operation of the device. For example, the RF emission generated by the electronic components of the device. It is well known in literature that electronic devices can release RF emissions containing information on the operation of the device, thus disclosing sensitive information and generating a security threat. This was one of the primary drivers for the definition of the TEMPEST (Telecommunication and Electronic Material Protected from Emanating Spurious Transmission) standard. TEMPEST refers to the possibility of spying on information systems through leaking emanations, including unintentional radio or electrical signals, sounds, and vibrations (see Rohatgi, P., (2009) for a description of the TEMPEST standard). This issue is also known as emission security (EMSEC), which is a subset of communications security (COMSEC). Since there is already a well-defined standard (i.e., TEMPEST) and a considerable amount of work in EMSEC and COMSEC for “unintentional” emissions, this chapter focuses only on the collection of fingerprints from “intentional” emissions, which are generated by the wireless device while performing its communication function or other services.

The main idea of identifying a wireless device through its RF emissions is that the electronic circuits and the RF components have specific characteristics determined by the production and manufacturing processes. These characteristics, which result in unique differences, can be used to distinguish a wireless device from another. The RF components can include filters, amplifiers, oscillators and other electronics, which are used to compose and transmit the RF signal. The differences on the electronic components are randomly generated, and are mainly due to imperfections in the material or the component itself. For example, the material can have impurities due to the presence of different substances or tiny differences in the soldering or casing of the amplifier, which have an impact in the generation of the RF emissions. These imperfections appear as a subtle modification of the RF signal in space even if the wireless device generates a signal conformant to the standard. For example, a GSM mobile phone can transmit a RF signal with the modulation and range of frequencies defined in the GSM standard, but the physical imperfections will produce minor changes in the amplitude or phase of the signal, which can be collected and processed by a receiver. Note that these minor changes will be substantially the same from statistical point of view in every transmission of the signal and they can be used as a fingerprint of the wireless component (and, consequently, of the GSM mobile phone). As it will be described in the following sections of this article, machine learning or signal processing techniques can be applied to the collected RF signal to extract the imperfections and the related fingerprints.

RF fingerprints can have many applications if the level of identification accuracy is high (e.g., 80-90% or more). The possibility of identifying wireless devices from their RF fingerprints can be used for multi-factor authentication, where a wireless device can be authenticated not only on the basis of conventional cryptographic methods but also by processing the RF fingerprints. Another potential application is to fight against the distribution of counterfeit products. Counterfeit wireless devices (e.g., mobile phones) have electronic components of worst quality in comparison to the genuine ones (Tehraniipoor et al., 2015). For example, if a counterfeit phone has been built with low grade RF amplifiers in the uplink transmission chain, it will generate different RF fingerprints compared to an original one.

The structure of this article is the following: the *Background* section provides the main definitions and a literature review on this topic. The section *RF fingerprinting methodology* describes the main workflow for the collection and processing of the RF signals to generate the fingerprints. It also highlights the main outstanding challenges. The section *Solutions and recommendations* identifies and describes the

11 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/identification-of-wireless-devices-from-their-physical-layer-radio-frequency-fingerprints/214672

Related Content

Developing a Theory of Portable Public Key Infrastructure (PORTABLEPKI) for Mobile Business Security

Sashi Nand (2009). *Mobile Computing: Concepts, Methodologies, Tools, and Applications* (pp. 2784-2791).

www.irma-international.org/chapter/developing-theory-portable-public-key/26692

A Deep Learning Approach for Detection of Application Layer Attacks in Internet

V. Punitha and C. Mala (2020). *Handling Priority Inversion in Time-Constrained Distributed Databases* (pp. 175-188).

www.irma-international.org/chapter/a-deep-learning-approach-for-detection-of-application-layer-attacks-in-internet/249430

Effects of Web Accessibility on Search Engines and Webometrics Ranking

Media Anugerah Ayu and Mohamed Ahmed Elgharabawy (2013). *International Journal of Mobile Computing and Multimedia Communications* (pp. 69-94).

www.irma-international.org/article/effects-web-accessibility-search-engines/76397

Mobile Government in Jordan: Is It a Step in the Right Direction?

Sultan Al-masaeed and Steve Love (2013). *International Journal of Handheld Computing Research* (pp. 93-116).

www.irma-international.org/article/mobile-government-in-jordan/84828

Apps, Apps, and More Apps: Motivations and User Behaviours

Matthew J. Haught, Ran Wei and Jack V. Karlis (2016). *International Journal of Mobile Computing and Multimedia Communications* (pp. 1-14).

www.irma-international.org/article/apps-apps-and-more-apps/148258