Security of IoT Devices in 5G Networks Through Fingerprinting and Side-Channel Analysis

Aurélien Francillon, Clémentine Maurice, Pierre Ayoub

November 14, 2020

Contents

1 Abstract

English For many years, 3rd and 4th generations of mobile networks have allowed users to receive service anywhere, at any time. The dawning and visionary 5th generation of mobile network (5G) aims to create a highly-decentralised architecture, including a massive Internet of Things (mIoT) and a non-federated core network, making telecommunications ubiquitous, faster, and safer. In order to achieve this last goal, many challenges must be addressed, in particular security concerning the hardware and software interface, as well as low-level hardware security issues due to electromagnetic emanations. This thesis aims at address some of these challenges, by a fingerprinting and side-channel attack approach.

Français Depuis de nombreuses années, les 3ème et 4ème générations de réseaux mobiles ont permis aux utilisateurs de recevoir un service téléphonique partout et à tout moment. Le 5ème génération de réseaux mobiles

(5G) vise à créer un réseau hautement décentralisé, incluant un Internet massif des objets (mIoT) et un cœur de réseau non fédérée qui rend les télécommunications omniprésentes, plus rapides et plus sécurisée. Pour atteindre ce dernier objectif, de nombreux défis doivent être relevés, notamment la sécurité concernant l'interface entre le matériel et le logiciel, ainsi que la sécurité bas-niveau du matériel dus aux émanations électromagnétiques. Cette thèse vise à relever certains de ces défis, par une approche de prise d'empreinte et d'attaque par canal auxiliaire.

2 Context

This Ph.D. will be conducted in the context of a collaboration between EURECOM (Sophia-Antipolis) and IRISA (Rennes) as part of the ANR project MobiS5 (the project also includes: Orange, Limoges University and Université Clermont Auvergne). The student will be located at Eurecom with visits in Rennes and Lille. MobiS5 aims to provide a security toolbox for 5G networks, validated formally and experimentally, responding to the needs of 5G networks at three levels:

- Security in the network infrastructure,
- Network access control,
- Security and privacy of end-user communications.

This Ph.D. is included in the MobiS5 project to propose a set of security solutions enabling end-to-end trust in the highly heterogeneous ecosystem of 5G.

3 State of the Art

Telecommunication systems have evolved a lot since their first usage in the 19th century, and the more time goes by the faster the evolution is. The new 5G network has a lot of promises to fulfill, with a lot of them regarding the security of the users. In parallel, radio technology has evolved, making radio attacks less costly and easier than before, in particular with the massive usage of Software Defined Radio (SDR), which allows a user to define his own radio signal processing using a software environment. The most important differences between current and future mobile networks are the virtualization and "softwarization" of the mobile core network, and the variety of devices requesting access to the network. In current mobile networks,

the Mobile Network Operator (MNO) has solely the responsibility to ensure the security of the mobile core network. The emergence of the network virtualization and softwarization aspect implies the emergence of new actors that may be involved in the assurance and maintenance of the network security. Consequently, it is crucial to ensure the security of those new actors.

On the first aspect, each IoT device (or class of devices) shows different characteristics both in terms of the software and physical components of the communication layers (e.g., application, transport, radio layers). Some of these characteristics (such as packet headers, traffic rate, radio waveforms) can be observable from the way the device communicates in the network. Using these features, it is often possible to uniquely identify devices with a so-called fingerprint, and to form a database of known and benign device identification information [Fra+06]. Using this database, one can later verify the identity of devices. This could also be used to authenticate the device and identify anomalies such as the use of the device by unauthorized parties.

On the second aspect, past research in the recent years still shows that despite the evolution of the protocols used in the mobile networks, the hardware is still a source of leakage and insecurity. The features selected for fingerprinting can also unintentionally leak information on computations, and therefore become side channels that can be exploited on the device. A recent research direction is the analysis of mixed-signal circuits [Cam+18] [CFS20], i.e., digital circuits and analog circuits on the same silicon die in close physical proximity, which is typically the case in low-cost devices found in IoT. In such designs, the processor's activity leaks into the analog portion of the chip, and can be recovered in the radio output. Such attacks have been demonstrated on low cost Bluetooth devices, but it remains to be evaluated if IoT devices in 5G are vulnerable and which other similar attacks or countermeasures may need to be considered. Mixed-signal chips side-channel attacks have also applications like audio eavesdropping [CYC20]. Rupprecht shows that the layer two of the protocols used in 4G and 5G are subject to integrity problems, leading to attacks like keystream reuse on some service (VoLTE) [Rup20]. Other integrity problems in some special message, like broadcast messages, could allow an attacker to perform a malicious signal injection [Yan+19].

4 Content

The topic of this Ph.D. is the security of end-devices from two complementary aspects: securing the network from malicious end-devices, and securing the

devices themselves.

For the fingerprinting work, the main challenges are:

1. Robustness, i.e., the system needs to be resilient against spoofing of the features, have high accuracy, and use stable features that will not depend on, *e.g.*, device's location, or distance from the network core,

2. Feature selection, as state of the art predominantly studied 802.11 frames at the *MAC* layer [Xu+16].

Finally, even if some features are possible to spoof, other features are harder to spoof, anti-fraud mechanisms can use this to detect some of the malicious devices.

We also observe that most of the devices in a 5G network could be subject to side-channel attacks. Indeed, an attacker will have physical access to stolen or lost personal devices and to a variety of small connected devices as surveillance cameras for instance. Moreover, the adversary may be able to make her own software run on smart devices (e.g. mobile app). Thus, the cryptographic primitives and protocols used should also be studied with regard to this specific kind of threats. In this thesis, we will look for new side-channel attacks on those algorithms and their potential mitigation. In order to assess the relevancy of those attacks (and the corresponding countermeasures), their impact in the particular context of 5G networks will be considered and experiments on representative hardware will be conducted.

We will first experiment those techniques on multiple IoT devices connected to a 4G network. Later, we will use an open source 5G testbed (OpenAirInterface [Nik+14], developed at EURECOM) and simulate device communications for our experiments.

References

[Cam+18] Giovanni Camurati et al. "Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers". In: *Proceedings of the 25th ACM conference on Computer and communications security (CCS)*. CCS '18. event-place: Toronto, Canada. ACM, Oct. 2018.

[CFS20] Giovanni Camurati, Aurélien Francillon, and François-Xavier Standaert. "Understanding Screaming Channels: From a Detailed Analysis to Improved Attacks". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES 2020)* 2020.3 (June 2020), pp. 358–401. DOI: 10.13154/tches.v2020.i3.358-401. URL: https://tches.iacr.org/index.php/TCHES/article/view/8594.

[CYC20] Jieun Choi, Hae-Yong Yang, and Dong-Ho Cho. "TEMPEST Comeback: A Realistic Audio Eavesdropping Threat on Mixed-Signal SoCs". In: *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. CCS '20. Virtual Event, USA: Association for Computing Machinery, 2020, pp. 1085–1101. ISBN: 9781450370899. DOI: 10.1145/3372297.3417241. URL: https://doi.org/10.1145/3372297.3417241.

[Fra+06] Jason Franklin et al. "Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting". In: *Proceedings of the 15th Conference on USENIX Security Symposium - Volume 15*. USENIX-SS'06. event-place: Vancouver, B.C., Canada. USA: USENIX Association, 2006.

[Nik+14] Navid Nikaein et al. "OpenAirInterface: A Flexible Platform for 5G Research". In: *ACM SIGCOMM Computer Communication Review* 44.5 (Oct. 10, 2014), pp. 33–38. ISSN: 0146-4833. DOI: 10.1145/2677046.2677053. URL: https://dl.acm.org/doi/10.1145/2677046.2677053 (visited on 11/14/2020).

[Rup20] David Rupprecht. "Enhancing the Security of 4G and 5G Mobile Networks on Protocol Layer Two". PhD thesis. Ruhr-Universität Bochum, May 2020.

[Xu+16] Qiang Xu et al. "Device Fingerprinting in Wireless Networks: Challenges and Opportunities". In: *IEEE Communications Surveys & Tutorials* 18.1 (2016), pp. 94–104. ISSN: 1553-877X. DOI: 10.1109/COMST.2015.2476338. URL: http://ieeexplore.ieee.org/document/7239531/ (visited on 11/14/2020).

[Yan+19] Hojoon Yang et al. "Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE". In: *Proceedings of the 28th USENIX Conference on Security Symposium*. SEC'19. event-place: Santa Clara, CA, USA. USA: USENIX Association, 2019, pp. 55–72. ISBN: 978-1-939133-06-9.