PhD position: "Security of IoT devices in 5G networks through fingerprinting and side-channel analysis"

Advisor: Aurélien Francillon (Eurecom, Sophia-Antipolis, France)
aurelien.francillon@eurecom.fr
Co-supervisor: Clémentine Maurice (CNRS, IRISA, Rennes, France)
clementine.maurice@irisa.fr

Context

This PhD will be conducted in the context of a collaboration between Eurecom (Sophia-Antipolis) and IRISA (Rennes) as part of the ANR project MobiS5[1] (the project also includes: Orange, Limoges University and Université Clermont Auvergne). The student will be located at Eurecom with visits in Rennes (frequency and duration to be discussed).

Description

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.

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

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 [1]. 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. 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 [3]. 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.

[1] https://mobis5.limos.fr

On the second aspect, the features that can be used to fingerprint these devices 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 [2], 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.

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, developed at EURECOM) and simulate device communications for our experiments.

Required skills

In this project we are looking for a curious and motivated student which has passion for research and technology with a background in Computer Science or Electrical Engineering. In particular, we are looking for a student with prior knowledge or an interest to learn: low level wireless physical layer, radio engineering (software defined radio...), software development, statistics and networking protocols.

Application

Candidates should send their CVs, references and motivation letters by mail to both Aurélien Francillon <aurelien.francillon@eurecom.fr> and Clémentine Maurice <clementine.maurice@irisa.fr>.
Position is open until filled. Possible starting date October 2018.

References

[1] Jason Franklin, Damon McCoy: Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting. USENIX Security Symposium 2006
http://static.usenix.org/event/sec06/tech/full_papers/franklin/franklin.pdf
[2] Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, Aurélien Francillon: Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers. ACM Conference on Computer and Communications Security 2018: 163-177
http://s3.eurecom.fr/docs/ccs18_camurati_preprint.pdf
[3] Qiang Xu, Rong Zheng, Walid Saad, Zhu Han: Device Fingerprinting in Wireless Networks: Challenges and Opportunities. IEEE Communications Surveys and Tutorials 18(1): 94-104 (2016)
https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7239531
[4] Navid Nikaein, Mahesh K. Marina, Saravana Manickam, Alex Dawson, Raymond Knopp, Christian Bonnet: OpenAirInterface: A Flexible Platform for 5G Research. Computer Communication Review 44(5): 33-38 (2014) https://www.openairinterface.org/