

# GIOVANNI CAMURATI

Digital Security Department, EURECOM, Sophia Antipolis, France  
Office 362, (+33)666316264, camurati@eurecom.fr

## KEY STRENGTHS

- Curious, proactive, and reliable. Patient, and considerate.
- All-round experience (research, collaborations, teaching, talks, international environment).
- Interplay of Hardware, Software, and Wireless, for Embedded Systems Security.

## HIGHLIGHTS

- Screaming Channels, a novel side channel (CHES 2020 paper, ACM CCS 2018 paper, Black Hat USA 2018 talk and other invited presentations, 3<sup>rd</sup> place in Europe at the CSAW 2018 Applied Research Competition, Google Bughunter Program Honorable Mention, covered by Le Monde and The Register). [http://s3.eurecom.fr/tools/screaming\\_channels/](http://s3.eurecom.fr/tools/screaming_channels/)
- Winner (academic team NOPS) at Hack@DAC 2019 contest on System-on-Chip security. <https://hack-dac19.trust-sysec.com/>

## EDUCATION and EXPERIENCE

- **EURECOM**, Sophia-Antipolis, France, **Sorbonne Université**, Paris, France  
Ph.D. Student (2017-Expected 2020)
- **Télécom-ParisTech**, Paris, France  
Diplôme d'Ingénieur (double MS degree with Politecnico di Torino, 2017)
- **Politecnico di Torino**, Turin, Italy  
MS, *cum laude*, Electronic Engineering (double degree with Télécom-ParisTech, 2017)  
BS, *cum laude*, Electronic Engineering (2014)
- **Arm**, Sophia-Antipolis, France  
Internship (July-December 2016)

## PUBLICATIONS

- **SoC Security Evaluation: Reflections on Methodology and Tooling**  
Nassim Corteggiani, Giovanni Camurati, Marius Muench, Sebastian Poeplau, Aurélien Francillon  
Accepted for publication in IEEE Design and Test, Special Issue on Hack@DAC
- **Understanding Screaming Channels: From a Detailed Analysis to Improved Attacks**  
Giovanni Camurati, Aurélien Francillon, François-Xavier Standaert  
IACR Transactions on Cryptographic Hardware and Embedded Systems. 2020, 3 (June 2020), 358-401
- **Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers**  
Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, Aurélien Francillon  
Proceedings of the 25th ACM conference on Computer and communications security (CCS), Toronto, Canada, October 2018 (acceptance rate: 16.6%)
- **Inception: System-wide Security Testing of Real-World Embedded Systems Software**  
Nassim Corteggiani, Giovanni Camurati, Aurélien Francillon  
Proceedings of the 27th USENIX Security Symposium (USENIX Security), Baltimore, USA, August 2018 (acceptance rate: 19.1%)

## SKILLS

- **Side Channel Attacks**
  - Theoretical background (e.g., preprocessing, statistical analysis).
  - Practical measurements (e.g., real-world targets, radio equipment).
  - Interplay of side-channel leakages and wireless transmissions in mixed-signal chips.
  - Discovery, analysis, and exploitation in realistic settings of a novel side channel vector: Screaming Channels. See [http://s3.eurecom.fr/tools/screaming\\_channels/](http://s3.eurecom.fr/tools/screaming_channels/).
- **Dynamic Security Analysis of Firmware**
  - Familiar with the main challenges (e.g., inline assembly, interrupts, peripherals).
  - Contributed to a novel approach: symbolic execution of a unified representation of high-level C/C++ code, inline ArmV7-M assembly, and processor behavior, while interacting with peripherals and interrupts on a real board through a custom debugger. See Inception <https://inception-framework.github.io/inception/>.
- **Security Analysis of a System-on-Chip**
  - Academic winner of the 2019 edition of Hack@DAC with the 4-person team NOPS.
  - Code and hardware design review, simulation of well-crafted tests, hardware fixes.
- **Computer Architectures and Digital Design**
  - Computer architectures (e.g., cache coherency).
  - Experienced with HDL (mostly VHDL, but also basic Verilog and SystemC).
  - Practical experience with a state-of-the-art multi-core processor (internship in Arm).
  - DLX processor with a windowed register file (2-person university project)
  - Several projects on FPGA, including a low-latency USB3-to-JTAG debugger.
- **Computer Science and Programming**
  - Extensive use of C, Python, ArmV7-M, Bash. Programming of microcontrollers. Basic/occasional use of C++, TCL, MATLAB and Simulink, x86 assembly.
  - Basic algorithms and data structures, multithreaded programming, practical networking for everyday tasks. Linux user (Arch Linux, Ubuntu).
- **Electronics**
  - Background in digital and analog electronics, laboratory equipment, measurements (e.g., design and calibration of a multimeter with custom analog circuits).
  - Basics of radio communications, and control science (e.g., line-follower robot).
- **Security Fundamentals:** wireless/hardware/system/software security and cryptography.
- **Other:** Some basics of project management and machine learning for personal interest.

## ACADEMIC SERVICE

- Reviewer, IEEE Transactions on Information Forensics & Security
- Poster/Demo Program Committee, ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) 2020
- Replicability Committee, ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSeC) 2019
- Reviewer, IEEE Design Automation & Test in Europe (DATE) 2019
- Reviewer, Smart Card Research and Advanced Applications (CARDIS) 2018

## TEACHING

- **VU Amsterdam**, Amsterdam, The Netherlands (remote from France)
  - Guest lecture “Wireless Security, a Brief Introduction” (2020/11/25).
- **EURECOM**, Sophia-Antipolis, France
  - Assistant for the Wireless Security course (2018-2021). Supervised around 20 different projects per year, plus other 6 semester projects since 2017.

## SELECTED COVERAGE

- **LE MONDE**, Les très indiscreètes puces des objets connectés (2018/07/25).  
[https://www.lemonde.fr/pixels/article/2018/07/25/les-tres-indiscretes-puces-des-objets-connectes\\_5335566\\_4408996.html](https://www.lemonde.fr/pixels/article/2018/07/25/les-tres-indiscretes-puces-des-objets-connectes_5335566_4408996.html)
- **The Register**, Boffins: Mixed-signal silicon can SCREAM your secrets to all (2018/07/27).  
[https://www.theregister.co.uk/2018/07/27/screaming\\_channels\\_attack/](https://www.theregister.co.uk/2018/07/27/screaming_channels_attack/)

## SELECTED TALKS

- **2019 Hack@DAC Top Finalist Team "NOPS" Presents their Approach**  
Design and Automation Conference (DAC) 2019, Las Vegas, USA (Designer track invited talk)
- **Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers**  
ACM CCS 2018, Toronto, Canada (Presentation of the paper)  
<https://youtu.be/OlafNH2WHxk>
- **Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers**  
Black Hat 2018, Las Vegas, USA (50-Minute Briefings, Giovanni Camurati, Marius Muench)  
<https://youtu.be/K7wqwOzD1Yw>
- **Invited talks about Screaming Channels at:**
  - Workshop on Practical Hardware Innovations in Security Implementation and Characterization (PHISIC) 2019, Gardanne, France
  - Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI) 2019, Erquy, France (in French)

## LANGUAGES

- **Italian**: native
- **English**: fluent; **Cambridge Certificate of Advanced English** (Level **C1** grade B)
- **French**: fluent; **DEL F A1-A2** in 2005, Level **C2** EU Language Assessment in 2016
- **Chinese**: currently learning Mandarin A1

## REFERENCES

- **Aurélien Francillon, Ph.D.**  
Associate Professor at EURECOM, Sophia-Antipolis, France  
[aurelien.francillon@eurecom.fr](mailto:aurelien.francillon@eurecom.fr), (+33) 493008119
- **Luciano Lavagno, Ph.D.**  
Full Professor at Politecnico di Torino, Turin, Italy  
[luciano.lavagno@polito.it](mailto:luciano.lavagno@polito.it), (+39) 0110904150
- **François-Xavier Standaert, Ph.D.**  
Professor at Université Catholique de Louvain, Louvain-la-Neuve, Belgium  
[fstandae@uclouvain.be](mailto:fstandae@uclouvain.be), (+32) 10472565