# GIOVANNI CAMURATI

Institute of Information Security, ETH Zurich, Zurich, Switzerland
Office CNB F102.1, giovanni.camurati@inf.ethz.ch

## 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, 3rd place in Europe at the CSAW 2018 Applied Research Competition, article in Encyclopedia of Cryptography, Security and Privacy, Google Bughunter Program Honorable Mention, covered by Le Monde and The Register). http://s3.eurecom.fr/tools/screaming_channels/.
- Runner-up Ph.D. Award from GDR Sécurité Informatique. https://gdr-securite.irisa.fr/prix-de-these/.

## EDUCATION and EXPERIENCE

- **ETH Zurich**, Zurich, Switzerland
  Postdoctoral Researcher (2021-ongoing)
- **EURECOM**, Sophia-Antipolis, France, **Sorbonne Université**, Paris, France
  Ph.D. (2017-2020)
- **Télécom-ParisTech**, Paris, France
  Diplôme d'Ingégneur (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

- **Time for Change: How Clocks Break UWB Secure Ranging**
  C. Anliker, G. Camurati, S. Capkun
  To appear at 32nd USENIX Security Symposium (USENIX Security), Anaheim, USA, 2023
- **EdgeTDC: On the Security of Time Difference of Arrival in CAN Bus Systems**
  M. Roechlin, G. Camurati, P. Brunner, M. Singh, S. Capkun
  Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, USA, 2023
- **MCRank: Monte Carlo Key Rank Estimation for Side-Channel Security Evaluations**
  G. Camurati, M. Dell'Amico, F.-X. Standaert
  IACR Transactions on Cryptographic Hardware and Embedded Systems. 2023, 1, 277-300
- **Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging**
  P. Leu*, G. Camurati*, A. Heinrich, M. Roeschlin, C. Anliker, M. Hollick, S. Capkun, J. Classen (*Equal contribution)
  Proceedings of the 31st USENIX Security Symposium (USENIX Security), Boston, USA, 2022

- **Noise-SDR: Arbitrary Modulation of Electromagnetic Noise from Unprivileged Software and Its Impact on Emission Security**
  G. Camurati, A. Francillon
  Proceedings of the 43rd IEEE Symposium on Security and Privacy (SP 2022), San Francisco, USA, May 2022
- **SoC Security Evaluation: Reflections on Methodology and Tooling**
  N. Corteggiani, G. Camurati, M. Muench, S. Poeplau, A. Francillon
  IEEE Design & Test. 2021, 38(1), 7-13
- **Understanding Screaming Channels: From a Detailed Analysis to Improved Attacks**
  G. Camurati, A. Francillon, F.-X. Standaert
  IACR Transactions on Cryptographic Hardware and Embedded Systems. 2020, 3, 358-401
- **Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers**
  G. Camurati, S. Poeplau, M. Muench, T. Hayes, A. Francillon
  Proceedings of the 25th ACM conference on Computer and communications security (ACM CCS), Toronto, Canada, October 2018 (acceptance rate: 16.6%)
- **Inception: System-wide Security Testing of Real-World Embedded Systems Software**
  N. Corteggiani, G. Camurati, A. Francillon
  Proceedings of the 27th USENIX Security Symposium (USENIX Security), Baltimore, USA, August 2018 (acceptance rate: 19.1%)

## SKILLS

- **Side Channel Attacks**
  - Theoretical background and practical measurements.
  - 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/.
  - Key ranking. See https://github.com/giocamurati/mcrank/.
- **Radio communications and Wireless Security**
  - Noise-based fully-digital radios. See https://github.com/eurecom-s3/noise-sdr/.
  - UWB distance measurements. See https://securepositioning.com/ghost-peak/.
  - Wireless Security.
- **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, while interacting with real hardware. 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).
- **Computer Science and Programming**
  - Extensive use of C, Python, ArmV7-M, Bash. Programming of microcontrollers. Basic/occasional use of C++, TCL, MATALAB 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 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

- PC Member, IEEE Symposium on Security and Privacy (SP) 2024
- PC Member, ACM Conference on Computer and Communications Security (CCS) 2023
- Reviewer, IEEE Transactions on Information Forensics & Security
- Poster/Demo Program Committee, ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) 2021
- 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

- **ETH Zurich**, Zurich, Switzerland (2021-now)
    - Assistant for Security of Wireless Networks (2021-2022, 2022-2023).
    - Assistant for Information Security Lab (2021-2022, 2022-2023).
    - Involvement in System Security and Seminar on Current Topics in Information Security (2022-2023).
    - Supervision of Master Theses and Student Projects.
- **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 indiscrètes 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
- **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/

## SELECTED TALKS

- **Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers**
  ACM CCS 2018, Toronto, Canada (Presentation of the paper)
  https://youtu.be/0IafNH2WHxk

- **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; **DELF 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, (+33) 493008119
- **Luciano Lavagno, Ph.D.**
  Full Professor at Politecnico di Torino, Turin, Italy
  luciano.lavagno@polito.it, (+39) 0110904150
- **François-Xavier Standaert, Ph.D.**
  Professor at Université Catholique de Louvain, Louvain-la-Neuve, Belgium
  fstandae@uclouvain.be, (+32) 10472565