

Nathanaël Denis

Mail:nathanael.denis@kaust.edu.sa

Individual notice

Current and previous situation

After a general engineering course at *Télécom SudParis, Polytechnic Institute of Paris* (Systems and Network Security Option), I carried out **a Ph.D. in Computer Science** within the same institution in the laboratory *SAMOVAR*, *RST department*, under the supervision of Professors Maryline Laurent and Sophie Chabridon.

I am **currently continuing my research activities** as **Postdoctoral Research Fellow** within the cybersecurity center (formerly RC3) at *King Abdullah University of Science and Technology* (KAUST), with Professor Roberto Di Pietro as *principal investigator*. My research interests align with the curiosity-driven research group and encompasses very diverse impactful topics including:

- Satellite cybersecurity
- Corrosion monitoring
- Drone security (physical and cyber)
- Electronics classification
- Quantum machine learning

As a result of the research performed at KAUST (two years): **6 accepted articles in top venues**, an additional 10 articles submitted and **2 patents being processed.**

Degrees

2020-2023 Ph.D. in Computer Science, Télécom SudParis, *Polytechnic Institute of Paris* (IP Paris).

Titled: For a private and secure Internet of things with usage control and distributed ledger technology

Defense date: October 3, 2023

Supervision: Maryline Laurent (director) and Sophie Chabridon (co-supervisor)

Composition of the jury:

- ➔ The *President* was Philippe Pucheral (Professor).
- ➔ The *Jury* was composed of Vincent Roca, Mawloud Omar (Professor) and Sara Tucci-Piergiovanni.

2017-2020 Engineering degree (Master 2), Télécom SudParis, Palaiseau, France. Systems and Network Security (SSR) major.

- The **Graduation Internship** is titled "*Securing a client-server architecture*", produced under the supervision of Maryline Laurent (school supervisor) and Benjamin Rivray (company supervisor). The internship consisted of strengthening an operating system, after an initial audit phase.
- The **Graduation Project** *"DEBSUCON-SSR: Distributed event-driven system combining data splitting and encryption*" produced under the supervision of Maryline Laurent.This end-of-studies project resulted in a scientific article published in an international conference with peer-reviewing (SECRYPT, ERA-CORE B)

2020 ESSI degree. ESSI training leads to obtaining the title of *Information Systems Security Expert*, French level 7 title, i.e., professional certifications – Degree obtained as part of the Systems and Network Security option at Télécom SudParis..

2014-2017 Preparatory Classes for "Grandes Ecoles" MPSI-MP Henri Wallon, Valenciennes. Computer Option. Second year valedictorian (MP). French CPGE (Classes Préparatoires aux Grandes Écoles) are two-year intensive undergraduate programs preparing students for entrance exams to prestigious French Grandes Écoles. They offer rigorous academic training in various fields such as science, humanities, and economics, aiming to groom students for success in competitive examinations.

Career

February-July 2020, End-of-study internship at MBDA France, focused on operating system security and auditing.

Languages

• French - Native language

• English – 980 TOEIC

• Russian – B2 CECR

Programming languages

- Java
- Python
- C
- Javascript/ Node.js
- Solidity - for blockchain smart contracts
- TLA+ - Modeling and model checking
- Slurm - High-performance computing
- Android Studio

Research activities

Ph.D. work

I completed my Ph.D. from 2020 to 2023 at Télécom SudParis (Institut Polytechnique de Paris), within the SAMOVAR laboratory and under the supervision of Maryline Laurent and Sophie Chabridon. The Ph.D. is entitled *For a private and secure Internet of things with usage control and distributed ledger technology,* and seeks to resolve security and privacy issues in the Internet of Things. To do this, I relied on different technologies, notably distributed registers and usage control.

Thesis abstract: IoT devices represent one of the major targets for malicious activities. The grounds for this are manifold: first, to reduce the cost of security, manufacturers may sell vulnerable products, leaving users with security concerns. Second, many IoT devices have performance constraints and lack the processing power to execute security software. Third, the heterogeneity of applications, hardware, and software widens the attack surface.As a result, IoT networks are subject to a variety of cyber threats. To counter such a variety of attacks, the IoT calls for security and privacy-preserving technologies.For privacy concerns, usage control grants the users the power to specify how their data can be used and by whom. Usage control extends classic access control by introducing obligations, i.e., actions to be performed to be granted access, and conditions that are related to the system state, such as the network load or the time.This thesis aims at providing answers to the challenges in the Internet of Things in terms of performance, security and privacy. To this end, distributed ledger technologies (DLTs) are a promising solution to Internet of Things constraints, in particular for micro-transactions, due to the decentralization they provide. This leads to three related contributions:1. a framework for zero-fee privacy-preserving transactions in the Internet of Things designed to be scalable;2. an integration methodology of usage control and distributed ledgers to enable efficient protection of users' data;3. an extended model for data usage control in distributed systems, to incorporate decentralized information flow control and IoT aspects. A proof of concept of the integration (2) has been designed to demonstrate feasibility and conduct performance tests. It is based on IOTA, a distributed ledger using a directed acyclic graph for its transaction graph instead of a blockchain. The results of the tests on a private network show an approximate 90% decrease in the time needed to push transactions and make access decisions in the integrated setting.

Peer-reviewed journals and conferences

Publications are given in the following format, in descending chronological order: authors, publication title, year, full title of journal or conference, DOI, Conference quality.

- Vincenzo Sammartino, **Nathanaël Denis**, Omar Ibrahim, Roberto Di Pietro, *Fight Drones with Drones: Detecting Aerial Perimeter Intrusion using Drone-mounted Microphones*, **31st European Symposium on Research in Computer Security, (ESORICS)**, 2026. ERA-CORE: A. Acceptance rate: 15%.
- Nathanaël Denis, Roberto Di Pietro, *A Review of Radar for Corrosion Monitoring in Structures: Technologies, Integration, and Future Research Directions*, 2026,**IEEE Transactions on Instrumentation and Measurement** DOI: https://doi.org/10.1109/TIM.2026.3690823, Impact factor: 5.9 (2026), Acceptance rate: 20.5%
- Nathanaël Denis, Roberto Di Pietro, *A harmonic radar approach to steel oxidation measurements using spectrogram classification*, 2026, **Measurement**, DOI: https://doi.org/10.1016/j.measurement.2026.120355, Impact factor: 5.6 (2026), Acceptance rate: 19%
- Nathanaël Denis, Roberto Di Pietro, *The Looming Privacy Challenges posed by Commercial Satellite Imaging: Remedies and Research Directions*, 2025, **IEEE Access**, DOI: https://doi.org/10.1109/ACCESS.2025.3588593, Impact factor: 3.6 (2026), Acceptance rate: 27%

- Nathanaël Denis, Roberto Di Pietro, *Replicating Human Immune System via Harmonic Radar: A Framework and Preliminary Results in Thwarting Cyber-physical Attacks*, 2025, **DSN 2025**, DOI: https://doi.org/10.1109/DSN-S65789.2025.00013, ERA-CORE A, Acceptance rate: 13%
- Nathanaël Denis, Sophie Chabridon, Maryline Laurent, *Bringing privacy, security and performance to the Internet of Things using IOTA and usage control (*Extended paper), 2024, **Annals of Telecommunications**, DOI: https://doi.org/10.1007/s12243-023-01005-1, Impact factor: 1.9 (2022)
- Nathanaël Denis, Maryline Laurent, Sophie Chabridon.*Integrating Usage Control into Distributed Ledger Technology for Internet of Things Privacy*. 2023, **IEEE Internet of Things Journal**. DOI: 10.1109/JIOT.2023.3283300.Impact Factor: 10.6 (JCR'22);
- Nathanaël Denis, Sophie Chabridon, Maryline Laurent. *Bringing Privacy, Security and Performance to the Internet of Things Through Usage Control and Blockchains.* **Privacy and Identity Management (IFIP)**, Springer, 2021, pp. 57-72. DOI: 10.5220/0009833204050414;
- Nathanaël Denis, Pierre Chaffardon, Denis Conan, Maryline Laurent, Sophie Chabridon, Jean Leneutre. *Privacy-preserving Content-based Publish/Subscribe with Encrypted Matching and Data Splitting*. 2020, Proceedings of the 17th International Joint Conference on e-Business and Telecommunications, ICETE 2020 - Volume 2: **SECRYPT**, DOI: 10.1007/978-3-030-99100-5_6, Rank: ERA-CORE B

Grants

- Small Translational Research Grant (sTRG) awarded for the project "*Miniaturized Harmonic Radar for Measurement and Detection of Corrosion*". **Award amount:** $89,694.00. **Project Duration:** 12 months

Communications in national conferences and workshops with reading committee

- Nathanaël Denis, Maryline Laurent, Sophie Chabridon., *A Decentralized Model for Usage and Information Flow Control in Distributed Systems***, Workshop on Privacy Protection (APVP 2023)**, Burgundy Franche-Comté, France, June 12 to 15, 2023;
- Nathanaël Denis, Sophie Chabridon, Maryline Laurent,*Bringing Privacy, Security and Performance to the Internet of Things using IOTA and Usage Control*, **Privacy Protection Workshop (APVP 2022)**, Châtenay-sur-Seine, France, June 13 to 16, 2022;
- Nathanaël Denis, Sophie Chabridon, Maryline Laurent,*Internet of Things: Combining Security, Privacy and Performance*, **Privacy Protection Workshop (APVP 2021)**, Remote presentation, June 15 to 17, 2021.

Presentations and seminars

- *Integrating Usage Control into Distributed Ledger Technology for Internet of Things Privacy*, **Seminar at Thales** (French electronics group), Palaiseau, France, June 8, 2023;
- *Integrating Usage Control into Distributed Ledger Technology for Internet of Things Privacy*, **Cybersecurity on a Plate (CoAP) Seminar**, joint between the CEA, Télécom SudParis and Thalès. Palaiseau, France, April 18, 2023;
- *Bringing Privacy, Security and Performance to the Internet of Things using IOTA and Usage Contro*l, **ACMES Seminar**, from the SAMOVAR laboratory. Lisses, France, December 13, 2021;
- *Insects, rust and computers, radar detection using harmonic signals,* **Team seminar in KAUST**, Thuwal, Saudi Arabia, December 8, 2024

Participation in scientific events

- Participation in summer/winter schools:
    - **EUROCORR 2025 Corrosion Summer School,** Challenges of corrosion, failure analysis, monitoring and maintenance. September 4 to 6, 2025;
    - **The Hi! PARIS Summer School 2022 on AI & Data for Science, Business and Society**, Palaiseau, July 4 to 7, 2022;

    - **The 3rd Future-IoT PhD School 2020 – IoT meets security,** Strasbourg (distance), October 5 to 7, 2020;
    - **Cyber in Saclay - Winter School in Cybersecurity,** Saclay (distance), February 8 to 12, 2021;
- Associate Researcher of the chair **Personal Information Values and Policies** from the *Institut Mines-Télécom (IMT)*. Presentations on Ph.D. work in this context, in front of the members of the chair;
- Member of the organizing committee of **the Workshop on Privacy Protection (APVP 2022),** I actively participated in the organization of the workshop and the sessions, in welcoming and transporting the people present at this workshop.
- KAUST 6G Summit (Thuwal, Saudi Arabia): Poster presentation on satellite role in 6G and satellite physical-layer authentication
- EFC Corrosion Summer School: Courses about our corrosion work and networking with the community.

Publications without peer review

- **Current Hot Topics in Data Protection - BDVA Position Paper**. Written with industrial (Atos, Huawei, etc.) and academic ((Eindhoven University of Technology, University of Amsterdam, etc.) partners within the *Big Data Value Association (BDVA)*

Teaching activities

As part of my Ph.D. at Télécom SudParis, I carried out several labs within the module *Filtering* taught during the final year of the engineering course (Master 2 level). For each of the works exhibited, the other lab participants and I carried out a first repetition (slightly longer than a lab itself) to correct and suggest improvements to these labs.

Public

The lab in the Filtering module is aimed at a diverse audience, made up of the following two classes:

- 3rd year engineering students (Master 2) from Télécom SudParis, Télécom Paris and Ecole Polytechnique who have chosen the specialty *Systems and Network Security* or the IP Paris master's degree;
- Specialized master's students *Cybersecurity of Essential Service Operators*, professionals in retraining with great diversity regarding profiles, including people new to programming or conversely very autonomous profiles.

Details of the labs

School year	Duration	Labs
2020-2021	19.5h	AWS Filtering Solutions, Layer 2 Filtering, NAT and Applications, Checkpoint NGFW
2021-2022	36h	Same
2022-2023	34.5h	Same

Content of the different courses

AWS Filtering Solutions: In this lab, students interact with (Linux) instances deployed on Amazon Web Services. Students must set up network filtering to authorize certain types of traffic (related to DNS, VPN, etc.) and above all authorize certain machines to interact in order to configure instances and retrieve information via APIs. This first lab serves as an introduction and does not require handling network hardware.

Filtering at level 2: In this second lab, students must filter traffic at the link layer (layer 2 of the OSI model). This first lab requires handling several types of hardware: cabling, router, PCs that interact with each other, web server, etc. which is a source of many potential errors including defective hardware. Students stage attacks,*e.g.*, ARP spoofing, to test their filters and their solutions.

Checkpoint - Next Generation Firewall (NGFW): Long and graded lab (10 hours, divided into two sessions of 5 hours or three sessions of 4 hours-4 hours-2 hours depending on the year), less difficult conceptually than the others for students, but which requires finding the right balance in terms of help for students, the lab being graded.

In this lab, students set up a firewall at the application level, in addition to an intrusion detection system (IPS) and network packet inspection (DPI).

NAT and applications: In this lab, students make indirect use of address translation (NAT) to set up filtering on network addresses. This lab is the most conceptually complicated, and often requires re-explaining the principles and purposes of this lab several times.

Additional content

Cybersecurity CTFs

- Root-me: https://www.root-me.org/ndenis?inc=score&lang=en (Top 1%)
- Cryptohack: https://cryptohack.org/user/LaPoche/
- Challenge Brigitte Friang
- European Cyber week CTF 2021
- 24h CyberRange CTF Challenge: https://www.cyber.airbus.com/cyberrange/ - Winning team 1st out of 10 teams of 40 participants

Additional contact links

- LinkedIn: www.linkedin.com/in/nathanaël-denis-a40b93151
- Researchgate: https://www.researchgate.net/profile/Nathanael-Denis
- Google Scholar: https://scholar.google.com/citations?user=Xe9uSu8AAAAJ&hl=en
- Github: https://github.com/nathanael-denis
- ORCID: https://orcid.org/0000-0003-3232-7449
- Personal website: https://nathanael-denis.owlstown.net/