Grégor Quétel

gquetel.fr · github.com/gquetel

Email: quetel.gregor@gmail.com
Mobile: +33 7 67 81 10 31

Profile

Cybersecurity PhD student interested in where machine learning and security meet, both using ML to build better defenses (like intrusion detection systems) and keeping ML systems themselves secure.

Education

- **Télécom Paris** — Palaiseau, France
  PhD in Computer Science — *Oct 2023 – Present*
- **University of Turku (EIT Digital Master School)** — Turku, Finland
  M.Sc. in Information and Communication Technology – Cybersecurity — *2022 – 2023*
- **Cyberschool, University of Rennes** — Rennes, France
  M.Sc. in Computer Science – Cybersecurity — *2021 – 2023*
- **University of Rennes** — Rennes, France
  B.Sc. in Computer Science — *2020 – 2021*
- **IUT de Vannes** — Vannes, France
  DUT in Computer Science – Software Engineering — *2018 – 2020*

Experience

- **Télécom Paris – ACES team** — Palaiseau, France
  PhD Student — *Oct 2023 – Present*
  - **Applicative intrusion detection**: Designing a new class of applicative data collector that captures real application behavior by instrumenting parser. Implemented the approach by developing gaur, to automatically instrument applications. *"Parser Instrumentation for Semantic-Aware Applicative Intrusion Detection", IFIP SEC 2026.*
  - **SQL attack detection dataset (Superviz25-SQL)**: Produced a high-quality, realistic and diverse SQL attack detection dataset, with a default experimental protocol providing detection methods as baselines. *"Superviz25-SQL: high-quality dataset to empower unsupervised SQL injection detection systems", ANUBIS, ESORICS 2025 International Workshop.*
  - **Cross-domain benchmark (Superviz26-SQL)**: Extended it into the first multi-domain benchmark measuring how ML detectors generalize under different transfer learning settings (cross-domain, concept drift, few-shot adaptation). *In submission process.*
  - **Domain generalization study**: Showed that the nature of the selected feature drives cross-domain transfer for ML-based intrusion detection: detection methods based on protocol-level features collapse under domain shift. *In submission process.*
- **CentraleSupélec – PIRAT team (ex CIDRE)** — Rennes, France
  Research Intern — *Feb 2023 – Jul 2023*
  - **Exploratory research**: Explored instrumenting parsers to produce semantic data for application-level intrusion detection. The results directly led to my current PhD.
- **SEE-D** — Vannes, France
  Software Engineering Intern — *Mar 2020 – Jun 2020*
  - **Monitoring application**: Developed a data collection application for the company's virtual machines (Python, Docker, MongoDB, Bash) and an internal React dashboard to visualize metrics.

Projects

- **Mini-rack homelab**: A small home cluster managed declaratively with NixOS, where the whole infrastructure is defined as code and self-hosts my personal services, such as a SNI proxy or a certificate authority.
- **Nix ecosystem contributions**: Maintain packages in nixpkgs (e.g. MLflow), and contribute to community projects such as nix-topology.
- **ScholarSec**: Web app that builds targeted Google Scholar queries filtered by cybersecurity conference venues, organized by CORE ranking tiers. scholarsec.gquetel.fr.
- **TLS Interception Security of Consumer Antivirus (2021 – 2022)**: Built a tool inspecting the TLS fields sent by antivirus clients performing TLS interception to verify whether TLS interception is conducted, and if so, how securely it is done.

Technical Skills

- **Machine Learning**: Deep learning and classical ML (PyTorch, scikit-learn), Natural Language Processing (Hugging Face, Sentence Transformers), model evaluation and benchmarking, experiment tracking (MLflow)
- **Infrastructure & IaC**: Infrastructure as code (Nix, Docker), containers and scheduling (Docker, Slurm), monitoring (Prometheus, Grafana), mesh networking (Tailscale, WireGuard)
- **Security**: Intrusion detection systems, TLS interception, certificate authorities / PKI (step-ca), network security
- **Linux & Unix tooling**: Everyday CLI administration (Git, tmux, ...), service management (systemd, nginx), ZFS storage
- **Programming**: Python, Bash, JavaScript (prior experience with C, Java)
- **Languages**: French (native), English (C1), German (A2)