# Tristan Bilot

Paris, FR | tristan.bilot@universite-paris-saclay.fr | (+33)771897506 | Website | LinkedIn | GitHub | Scholar

## Education

**Ph.D. in Computer Science**, Université Paris-Saclay, Paris, France — 2022 – 2025 (expected)
- Thesis: Detecting Advanced Cyberattacks with Self-Supervised Graph Learning
- Supervisors: Pr. Khaldoun Al Agha, Nour El Madhoun

**Master's (Diplôme d'Ingénieur) in Computer Science**, EPITA, Paris, France — 2019 – 2022
- GPA: 4.0/4.0
- Focus on Computer Security, Systems, Network

**DUT in Computer Science**, Université Paris-Cité, Paris, France — 2017 – 2019
- Focus on Algorithms, Data Structures, Data Mining, Reflective Programming

## Experience

**Applied Scientist Intern** – Amazon AWS, New York, NY, USA — Oct. 2025 – Jan. 2026
- Research on LLM security

**Ph.D. Researcher** – Iriguard, LISN, LISITE, Paris, France — Oct. 2022 – Oct. 2025
- Ph.D. funded by Iriguard and in collaboration with LISN and LISITE labs
- Developed scalable intrusion detection systems with deep learning on client data

**Visiting Research Student** – University of British Columbia, Vancouver, BC, Canada — Apr. – Jun. 2024
- Research in provenance-based intrusion detection systems with GNNs and self-supervised learning, supervised by Thomas Pasquier
- Worked on large-scale temporal graphs and robustness to adversarial attacks

**Student Researcher** – EPITA Systems Laboratory (LSE), Paris, France — Sep. 2021 – Aug. 2022
- Research on GNNs for phishing web page detection, supervised by Dr. Badis Hammi

**Data Engineer Apprentice** – Carrefour-Google AI Lab, Paris, France — May 2021 – Aug. 2022
- Deployed ML models in production and optimized training time (4x and 3x improvements)
- Built a scalable BigQuery fetching tool, presented in internal engineering reviews
- Deployed a multi-project data pipeline with Airflow, dbt, GCP, Kubernetes

**Software Engineer Apprentice** – Carrefour, Paris/Massy, France — Sep. 2019 – Apr. 2021
- Developed new features for the Carrefour iOS app (1.5M+ monthly users)
- Integrated Apple Wallet into the app

**Software Engineer Intern** – Micropole, Levallois-Perret, France — May 2019 – Aug. 2019
- Developed backend features for websites and web services
- Improved website loading speed by ∼30%

## Publications

**Full list: Google Scholar**

KRATOS: Temporal Graph Transformer for Large-Margin Provenance-based Intrusion Detection — To be submitted
Tristan Bilot, Baoxiang Jiang, Nour El Madhoun, Khaldoun Al Agha, Anis Zouaoui, Thomas Pasquier — 2026

FAUCON: Targeted Lateral Movement Detection in Evolving Networks Through Source Host Identification — Submitted, USENIX Security
Tristan Bilot, Nour El Madhoun, Khaldoun Al Agha, Anis Zouaoui — 2026

Sometimes Simpler is Better: A Comprehensive Analysis of State-of-the-Art Provenance-Based Intrusion Detection Systems [paper, code, poster] — USENIX Security

Tristan Bilot, Baoxiang Jiang, Zefeng Li, Nour El Madhoun, Khaldoun Al Agha, Anis Zouaoui, Thomas Pasquier — 2025

ORTHRUS: Achieving High Quality of Attribution in Provenance-based Intrusion Detection Systems [paper, code] — USENIX Security
Baoxiang Jiang, Tristan Bilot, Nour El Madhoun, Khaldoun Al Agha, Anis Zouaoui, Shahrear Iqbal, Xueyuan Han, Thomas Pasquier — 2025

Few Edges Are Enough: Few-Shot Network Attack Detection with Graph Neural Networks [paper, code, slides] — IWSEC (**best paper award**)
Tristan Bilot, Nour El Madhoun, Khaldoun Al Agha, Anis Zouaoui — 2024

A Survey on Malware Detection with Graph Representation Learning [paper] — ACM Computing Surveys
Tristan Bilot, Nour El Madhoun, Khaldoun Al Agha, Anis Zouaoui — 2024

A Benchmark of Graph Augmentations for Contrastive Learning-Based Network Attack Detection with Graph Neural Networks [paper, poster] — CSNet
Tristan Bilot, Nour El Madhoun, Khaldoun Al Agha, Anis Zouaoui — 2023

Graph Neural Networks for Intrusion Detection: A Survey [paper] — IEEE Access
Tristan Bilot, Nour El Madhoun, Khaldoun Al Agha, Anis Zouaoui — 2023

PhishGNN: A Phishing Website Detection Framework using Graph Neural Networks [paper, code, slides] — SECRYPT
Tristan Bilot, Grégoire Geis, Badis Hammi — 2022

## Technical Articles

**USENIX ;login:** [article] — 2025
Article based on our two USENIX Security 2025 papers

**Medium** [11 articles + code] — 2020–now
Various articles on MLX/CUDA benchmarks, data eng., software eng., ...

**Personal Blog** [5 articles, code] — 2022
"Deep learning from scratch" series, on autodiff & backpropagation

## Talks

**GenAI Meetup Morocco** [slides] — Morocco – 2025
How AI protects us from cyberattacks?

**EPITA Seminar** [slides] — France – 2025
Introduction to ORTHRUS and PIDSMAKER

**University of Bristish Columbia** [slides] — Canada – 2024
Inductive Detection of Hosts in Large Temporal Graphs

**Institut Mines-Télécom** [slides] — France – 2024
System-level Intrusion Detection with Graph Neural Networks

**DATAIA Day Saclay** [poster] — France – 2022
Detecting Complex Attacks with Graph Deep Learning

**EPITA & Carrefour** [slides] — France – 2022
Data Engineering Applied to Retail

## Skills

**Programming:** Python, Swift, C, C++, Bash, JS, Java, CUDA, Assembly x86, Rust
**ML Frameworks:** PyTorch, MLX, Jax/Haiku, pandas, scikit-learn
**ML Skills:** Self-supervised learning, GNNs, Transformers, LLM fine-tuning (LLaMA+QLoRA), GPU parallelization & vectorization, framework coding, large-scale training under limited resources
**Infrastructure:** GCP, AWS, Docker, Kubernetes, Airflow, dbt, W&B
**Languages:** French (native), English (fluent), Spanish (notions)

## Projects

**PIDSMaker**, github.com/ubc-provenance/PIDSMaker 2025–
Deep learning framework for building provenance-based intrusion detection systems

**Apple MLX**, github.com/ml-explore/mlx 2024–
Apple's ML framework – Implemented backpropagation of scattering operations in C++

**MLX-graphs**, github.com/mlx-graphs/mlx-graphs 2024–
GNN library on top of MLX with optimized GPU kernels

**MLX-benchmark**, github.com/TristanBilot/mlx-benchmark 2024–
Benchmark framework for MLX, Apple chips and CUDA GPUs

**Deepiler**, github.com/TristanBilot/deepiler 2022
Transformer-based decompiler to convert binaries into C code

**K – x86 Kernel**, github.com/TristanBilot/kernel_x86 2021
Simple kernel written in C and Assembly x86

## Activities & Interests

**Volunteering:** Protection civile (2018–2022), first aid
**Academic:** Student bureau, Junior Entreprise, class representative, hackathons (Google HashCode, Design4Green, Carrefour)
**Hobbies:** Music (DJ mix), cosmology, traveling, surfing