Tristan Bilot

Paris, FR | Email | Website | LinkedIn | GitHub | Google Scholar

Education

Ph.D. in Computer Science, Université Paris-Saclay, Paris, France 2022 – 2025

- Thesis: Detecting Advanced Cyberattacks with Self-Supervised Graph Learning
- Supervisors: Pr Khaldoun Al Agha, Dr 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

Postdoctoral Fellow – University of British Columbia, Vancouver, BC, Canada Feb. 2026 –

- Research on foundation models for security

Applied Scientist Intern – Amazon, New York, NY, USA Oct. 2025 – Jan. 2026

- Security Analytics and Artificial Intelligence Research team (SAAR) at AWS
- Research on multi-agent system 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 + optimized training time (4x and 3x faster)
- 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 – *AR: Acceptance Rate*

PIDSMaker: Building and Evaluating Provenance-based Intrusion Detection Systems *Under review, KDD 2026* [preprint]

Tristan Bilot, Baoxiang Jiang, Thomas Pasquier

Kratos: Temporal Graph Transformer for Large-Margin Provenance-based Intrusion Detection — *Under review, S&P 2026*

Tristan Bilot, Baoxiang Jiang, Nour El Madhoun, Khaldoun Al Agha, Anis Zouaoui, Thomas Pasquier

Faucon: Targeted Lateral Movement Detection in Evolving Networks Through Source Host Identification — *Under review, USENIX Sec. 2026*

Tristan Bilot, Nour El Madhoun, Khaldoun Al Agha, Anis Zouaoui

Sometimes Simpler is Better: A Comprehensive Analysis of State-of-the-Art Provenance-Based Intrusion Detection Systems — *USENIX Security 2025 (AR: 17.1%)* [paper, code, poster, slides, video]

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

Orthrus: Achieving High Quality of Attribution in Provenance-based Intrusion Detection Systems — *USENIX Security 2025 (AR: 17.1%)* [paper, code, slides, video]

Baoxiang Jiang, Tristan Bilot, Nour El Madhoun, Khaldoun Al Agha, Anis Zouaoui, Shahrear Iqbal, Xueyuan Han, Thomas Pasquier

Few Edges Are Enough: Few-Shot Network Attack Detection with Graph Neural Networks — *IWSEC 2024 (AR: 29.8%), **best paper*** [paper, code, slides]

Tristan Bilot, Nour El Madhoun, Khaldoun Al Agha, Anis Zouaoui

A Survey on Malware Detection with Graph Representation Learning — *ACM Computing Surveys, 2024* [paper]

Tristan Bilot, Nour El Madhoun, Khaldoun Al Agha, Anis Zouaoui

A Benchmark of Graph Augmentations for Contrastive Learning-Based Network Attack Detection with Graph Neural Networks — *CSNet 2023* [paper, poster]

Tristan Bilot, Nour El Madhoun, Khaldoun Al Agha, Anis Zouaoui

Graph Neural Networks for Intrusion Detection: A Survey — *IEEE Access, 2023* [paper]

Tristan Bilot, Nour El Madhoun, Khaldoun Al Agha, Anis Zouaoui

PhishGNN: A Phishing Website Detection Framework using Graph Neural Networks — *SECRYPT 2022* [paper, code, slides]

Tristan Bilot, Grégoire Geis, Badis Hammi

Technical Articles

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

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

Personal Blog – “Deep learning from scratch” series, on autodiff & backpropagation — 2022 [5 articles, code]

Invited Talks

Télécom Paris – Course on AI techniques for advanced attack detection	France – 2026	[slides]
The University of Texas at El Paso – Achieving High Quality of Attribution in IDS	USA – 2025	[slides]
GenAI Meetup Morocco – How AI protects us from cyberattacks?	Morocco – 2025	[slides]
EPITA Seminar – Introduction to Orthrus and PIDSMaker	France – 2025	[slides]
University of British Columbia – Inductive Host Detection in Large Temp. Graphs	Canada – 2024	[slides]
Institut Mines-Télécom – System-level IDS with Graph Neural Networks	France – 2024	[slides]
DATAIA Day Saclay – Detecting Complex Attacks with Graph Deep Learning	France – 2022	[poster]
Carrefour – Data Engineering Applied to Retail	France – 2022	[slides]

Projects

PIDSMaker – Deep learning framework for building provenance-based IDS — 2025– [code]

Apple MLX – Implemented backpropagation of scattering operations in C++ — 2024– [code]

MLX-graphs – GNN library on top of MLX with optimized GPU kernels 2024– [code]

MLX-benchmark – Benchmark framework for MLX, Apple chips and CUDA GPUs 2024– [code]

Deepiler – Transformer-based decompiler to convert binaries into C code 2022 [code]

K – x86 Kernel – Simple kernel written in C and Assembly x86 2021 [code]

Skills

Programming: Python, Swift, C, C++, Bash, JS, Java, CUDA, Assembly x86, Rust
ML Frameworks: PyTorch, MLX, Jax/Haiku, pandas, scikit-learn
Agentic AI: Autogen/AG2, AWS Bedrock, LangChain, LangGraph
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)

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