Léo Lavaur

IMT Atlantique, Rennes, France | (+33) 7 88 26 99 22

linkedin.com/in/leolavaur
github.com/phdcybersec
contact@leolavaur.re
leolavaur.re

Postdoc position in Cybersecurity

Ph.D. Research

Doctoral Researcher 2020–*present*
IMT Atlantique, Rennes, France

Improving Intrusion Detection in Distributed Systems with Federated Learning.

Research work on collaborative intrusion detection supported by federated learning techniques. Study of its limits in terms of heterogeneity and resistance to poisoning, with construction of countermeasures. Work on dataset generation for distributed systems. Teaching, conferences and popularisation. Ph.D. directed by Pr. Yann Busnel and co-supervised by Fabien Autrel and Marc-Oliver Pahl. Project founded by the industrial chair CyberCNI.

Keywords: machine learning, federated learning, intrusion detection, collaboration, heterogeneous data, trust.

Education

Masters in Engineering, Information Security 2017–2020
ENSIBS, Vannes, France (rank: top 10, work-study program)

Two-year University Degree (DUT), Computer Science 2015–2017
IUT de Nantes, Nantes, France (rank: 2nd, work-study program)

Professional Experience

Orange Cyberdefense, Rennes, France 2017–2020
Three-year apprenticeship in the consulting division.

- **R&D Engineer** 2019–2020
  End-of-study Project on WI-FI network security and geolocation of malicious access points. Literature review, empirical studies, construction of a modular UAV prototype and a dedicated probe.
- **Application Security Analyst** 2017–2019
  Performing white box code audits using tools, sorting false positives and helping with correction. Development of internal tools for task automation.

Co-organizer (independent) 2019
RedHack CTF, Barcelona, Spain

International Capture The Flag (CTF) competition during the Barcelona Cybersecurity Congress. Realistic network infrastructures totaling more than 400 virtual machines.

Skills

Machine Learning

Building and training models, data preprocessing, evaluation, and visualization (PCA). TensorFlow/Keras for deep learning, scikit-learn for classical machine learning, Flower for federated learning. Daily use of data analysis libraries (pandas, numpy, matplotlib).

Tooling

Daily use of Git, Nix, and Linux & Unix systems. Past experience with Docker, Kubernetes, Ansible, and GitLab CI/CD.

Programming Languages

Proficient in Python and bash; knowledgeable in Go, Rust, C/C++, Java, JavaScript, HTML/CSS.

Security

Network protocols and security mechanisms, penetration testing, application security.

Languages

English (fluent, TOEIC 990/990).
French (native, 819/1000 at *Projet Voltaire*).

Intern Supervision

2024: *Gabriel Bourgeois*, “Analyse de la réutilisabilité de calcul dans un contexte d’apprentissage fédéré pour la détection d’intrusion”, Master 2 at UCAQ (Canada) / UTC (France), 6 months.
2023: *Akshat Chaudhary*, “Performance evaluation of FL for IDS”, Bachelor at IIT (India), 2 months.

Other achievements

- **Reviewer** for international venues: JNSM, TNSM, Computer Networks.
- **Tutorial host** at renowned international conferences: Network of the Future (NoF) 2023 [9], IEEE ICDCS 2024 [4].
- TPC member for RESSI 2023, **TPC co-chair** RESSI 2024.

- **Presentations** and posters at national venues: ECW, RESSI, Journées thématiques of GDR RSD, IMT's Cybersecurity & Risks seminar (best poster award, ex-aequo).
- Participation to national events: ECW, Journées thématiques of GDR RSD and GDR Sécurité, RESSI, AlgoTel/cores.
- **Scientific mediation** at France Culture (National-wide French radio): "Apprentissage Fédéré et Collaboratif pour combattre les cyber-attaques", in *La recherche montre en main, La Méthode Scientifique*, France Culture, 2022, postcast available at 48"30'

Publications

Journal articles

[1] **Léo Lavaur**, Marc-Oliver Pahl, Yann Busnel, and Fabien Autrel. "The Evolution of Federated Learning-based Intrusion Detection and Mitigation: A Survey". In: *IEEE Transactions on Network and Service Management*. Special Issue on Network Security Management (June 2022).

International conference papers

[2] **Léo Lavaur**, Pierre-Marie Lechevalier, Yann Busnel, Romaric Ludinard, Géraldine Texier, and Marc-Oliver Pahl. "RADAR: Model Quality Assessment for Reputation-aware Collaborative Federated Learning". In: *Proceedings of the 43rd International Symposium on Reliable Distributed Systems (SRDS)*. Charlotte, NC, USA, Sept. 2024.

[3] **Léo Lavaur**, Yann Busnel, and Fabien Autrel. "Systematic Analysis of Label-flipping Attacks against Federated Learning in Collaborative Intrusion Detection Systems". In: *Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES). Workshop on Behavioral Authentication for System Security (BASS)*. Vienna, Austria, Aug. 2024.

[4] Yann Busnel and **Léo Lavaur**. "Tutorial: Federated Learning × Security for Network Monitoring". In: *Proceedings of the 44th International Conference on Distributed Computing Systems (ICDCS)*. Jersey City, NJ, USA, July 2024.

[5] **Léo Lavaur**, Yann Busnel, and Fabien Autrel. "Demo: Highlighting the Limits of Federated Learning in Intrusion Detection". In: *Proceedings of the 44th International Conference on Distributed Computing Systems (ICDCS)*. Jersey City, NJ, USA, July 2024.

National venue papers

[6] **Léo Lavaur**, Pierre-Marie Lechevalier, Yann Busnel, Marc-Oliver Pahl, and Fabien Autrel. "Metrics and Strategies for Adversarial Mitigation in Federated Learning-based Intrusion Detection". In: *Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI)*. Neuvy-sur-Barangeon, France, May 2023.

[7] **Léo Lavaur**, Benjamin Coste, Marc-Oliver Pahl, Yann Busnel, and Fabien Autrel. "Federated Learning as Enabler for Collaborative Security between Not Fully-Trusting Distributed Parties". In: *Proceedings of the 29th Computer & Electronics Security Application Rendezvous (C&ESAR)*. Rennes, France, Oct. 2022.

[8] **Léo Lavaur**, Marc-Oliver Pahl, Yann Busnel, and Fabien Autrel. "Federated Security Approaches for IT and OT". In: *Journée thématique du GT sur la Sécurité des Systèmes, Logiciels et Réseaux (GT-SSLR)*. May 2021.

Tutorials

[9] Yann Busnel and **Léo Lavaur**. "Federated Learning × Security for Network Management". 15th International Conference on Network of the Future (NoF). Izmir, Turkey, Sept. 2023.

[10] Yann Busnel and **Léo Lavaur**. "L'interêt de l'apprentissage fédéré dans le cadre de la détection d'incidents sur les réseaux et/ou systèmes à grande échelle". Ecole de Printemps Recherche de l'EUR CyberSchool. Rennes, France, Apr. 2023.

Teaching

Practical sessions and exercises for Masters students in Computer Science at IMT Atlantique. Test and animation of a MOOC.

2022–2023

- "Basics of Network Security" (IPSec, 802.1X, Cisco ACLs, DNSSec, SSL/TLS), 16h
- "IoT Security" (Vulnerabilities, Network protocols exploitation), 10h
- "Basics of Networking" (Ethernet, IP, routing), 10h
- "Blockchain: challenges and cryptographic mechanisms (MOOC)" (Blockchain, Proof-of-Work vs. Proof-of-Stake, Bitcoin, SHA-256, ECDA), 64h

2021–2022

- "Basics of Network Security" (IPSec, 802.1X, Cisco ACLs, DNSSec, SSL/TLS), 24h
- "Basics of Network Security" (IPSec, 802.1X, Cisco ACLs, DNSSec, SSL/TLS), 16h
- "IoT Security" (Vulnerabilities, Network protocols exploitation), 10h
- "Network Intrusion Detection" (IDS principles, Suricata), 4h
- "Network Supervision" (SIEM principles, Prelude), 4h

Volunteering & Hobbies

- ENSIBS Alumni (board member), 2020–2023.
- Student associations (IUT de Nantes, ENSIBS).
- Capture The Flag competitions (1st BreizhCTF 2023, 3rd FakeNewsCTF 2022, 2nd EsaipCTF 2021).
- Sport (mountain biking, rock climbing, running).
- Computer Science (homelabing, automation).
- Œnology (whisky).