Jan Lauinger

PhD Candidate, Technical University of Munich, Germany
jp@ianzn.com — +49 (179) 2638-246 — Github — Personal Page — Google Scholar — TUM Profile

EDUCATION

Technical University of Munich (TUM), Germany — 10 2013 — 09 2016
Bachelor of Science Electrical and Computer Engineering — Overall Grade: 2.4
Thesis: Large Scale Anomaly Detection Using Spark (1.3), PDF

Technical University of Munich (TUM), Germany — 10 2016 — 09 2018
Master of Science Electrical and Computer Engineering — Overall Grade: 2.1
Thesis: Runtime System Adaptation in Web of Things (1.0), PDF

Technical University of Munich (TUM), Germany — 06 2019 — 04 2024
PhD (Dr.-Ing.) Electrical and Computer Engineering — Submitted 09 2024
Dissertation: Advancing Privacy-Enhancing Technologies for Policy-Driven Data Sovereignty and Provenance, PDF
Supervisors: 1st Prof. Steinhorst, 2nd Prof. Gervais, 3rd TBD

INDUSTRY EXPERIENCE

Internship Porsche AG — Weissach, Germany
Assistant in the Electronics Integration Centre (EIC) — 09 2014 — 10 2014

- Participation in different development sections.

Zaha Hadid Architects — London, England
Software Developer — 03 2015 — 04 2015 and 09 2015 — 10 2015

- Developer of software add-on for current program of kinematics solver.
- Add-on enabled parameter compatibility between the kinematic solver program and Robot Studio.

TUM Chair for IT Security — Munich, Germany
Research Assistant (HiWi) — 09 2016 — 03 2017

- Software developer: Shodan service integration (Holmes Totem) for IoT data discovery.
- Software developer: AI-based malware analysis using Apache Spark, Cassandra, and Livy.

TUM Chair of Network Architectures and Services — Munich, Germany
Research Internship (Forschungspraxis) — 04 2017 — 10 2017

- Evaluation of client discrimination in anonymization networks using active network scans.
- Project report as PDF.

EU's Horizon 2020 Research and Innovation Programme, project nIoVe (ga. no. 833742) — Europe
Management and Consulting (work package lead), Software Developer (deliverable lead) — 05 2019 — 09 2022

Deliverable lead:

- Quality assurance plan and report
- CAVs Cybersecurity threats digest and analysis
- Trust management and Identification platform. Leading to papers GIoTS20 and ICBC21 (see publications below).
- IoV ecosystem response toolkit & Recovery toolkit. Leading to papers DATE22, VTC22, VTC23 (see publications below) and toolkits *agf* and *iov_irs* (see coding repositories below).
- Threat Intelligence Repository

Work package lead:

- Secure Cyber-Threat Data Collection & Pre-processing across the CAVs Ecosystem

ACADEMIC EXPERIENCE

Research Associate (PhD Student) — TUM Associate Professorship of Embedded Systems and IoT (Munich, Germany)
Employment Time — 06 2019 — 04 2024
My academic experience involves the following activities:

- Teaching of masters **subject**: System Design for the Internet of Things 2019, 2020, 2021, 2022
- Teaching of masters **subject**: Scientific seminar embedded systems and IoT 2020, 2021, 2022, 2023, 2024
- Student supervision (9x master's thesis, 4x bachelor's thesis, 7x research internship), see further details here.
- Research and publications
- Dissertation writing and publication

TALKS

Given at international research conferences, industry events, and academic events:

- 2021 ICBC (Sydney): Paper presentation, A-PoA (slides).
- 2022 DATE ASD (Antwerp): Paper presentation, Attack data generation framework.
- 2023 Euro S&P (Delft): Paper presentation, SoK Data Sovereignty (slides, video).
- 2023 TUM Blockchain Salon (Garching): Decentralized Identity Management (slides, youtube).
- 2024 TUM Blockchain Salon (Garching): Transpiling Policies to Secure Computation Circuits (slides, youtube).
- 2024 ICBC (Dublin): Paper presentation, zkGen (slides).
- 2024 ICBC (Dublin): Paper presentation, Portal (slides).
- 2024 TUM Blockchain Conference (Munich): ZK 101 - The Magic of Proving Without Revealing (slides).
- 2025 PETS (Washington DC): Paper presentation, Janus.

OPEN-SOURCE CODING REPOSITORIES

- **gnark_lib**: Zero-knowledge circuit library for the gnark framework (e.g. dynamic AES128 in GCM mode with Plonk lookups). Includes ZKP verification at Ethereum smart contracts. **software** - Go, Solidity, go-ethereum, gnark
- **origo**: Command line toolkit to run and deploy 2PC-free TLS data provenance (zkTLS). **software** - Go
- **janus_artifacts**: MPC, FHE, and ZKP building blocks for efficient verification of data provenance. **software** - Go, go-mpc, gnark, go-crypto/tls
- **webstack1**: Modern go-based web stack for backend and frontend development (in action). **software** - Go, HTML, Javascript
- **kubehorizon**: Bare metal cluster with reverse-proxy load balancing for multi-service scaling.**software** - kubeadm, kubectl, MetalLB, Containerd, Debian, Go, Let's Encrypt, Postgres
- **kuberely**: High-availability cluster for single service scaling. **software** - kubeadm, kubectl, Go, Debian, Ansible
- **web3knowledge**: A collection of papers, courses, tools, researchers, and events.
- **iov_irs**: Internet of Vehicles (IoV) Intrusion Response System (IRS) using distributed workers. **software** - Python, Tornado, Celery asynchronous jobs, Svelte UI, RabbitMQ, MongoDB, Docker compose
- **agf**: Attack data generation framework for autonomous vehicle (AV) sensors (implements attacks and countermeasures). **software** - Python, Carla AV simulator, Tornado, MongoDB, Docker compose, Svelte UI, websockets
- **zkGen**: JSON policy to ZKP circuit transpiler. **software** - Go, gnark
- **portal**: Decentralized identity system with enhanced privacy (zk credentials) and control for users. Compliant with W3C standardizations of Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). **software** - Go, go-ethereum, gnark, Solidity

SKILLS SUMMARY

- **Communication:** English, German
- **Programming:** Go, Python, Javascript, C, Matlab, HTML, SQL, Solidity, CSS, Typescript, Latex, Apache Spark, MPC and ZKP domain specific languages (DSLs)
- **Software Frameworks/Tooling:** Gnark, Kubernetes, Docker, Linux, Ansible, Postgres, MongoDB, Cassandra, Cockroach, Svelte, Word, Excel, Powerpoint, Confluence, Google workspace, Overleaf, Mailcow, Hardhat
- **Cloud Administration:** AWS, Digital Ocean, Azure, Hetzner, Cloudflare, Godaddy, Let's Encrypt
- **Soft Skills:** Friendly, good attitude, collaboratively working, negotiating, planning, independent problem solving

PUBLICATIONS

Conference proceedings[1]

- J. Ernstberger*, J. **Lauinger***, Y. Wu, and S. Steinhorst, "Origo: Proving provenance of sensitive data with constant communication," (Washington, DC, USA), pp. 1–17, 2025
- J. **Lauinger**, J. Ernstberger, A. Finkenzeller, and S. Steinhorst, "Janus: Fast privacy-preserving data provenance for tls," in *The 25th Privacy Enhancing Technologies Symposium*, (Washington, DC, USA), pp. 1–20, 2025
- J. **Lauinger**, S. Bezmez, J. Ernstberger, and S. Steinhorst, "Portal: Single sign-on with time-bound and replay-resistant proofs," in *First IEEE International Workshop on Programmable Zero-Knowledge Proofs for Decentralized Applications (ZKDAPPS 2024)*, pp. 1–7, IEEE, 2024
- J. **Lauinger**, J. Ernstberger, and S. Steinhorst, "zkgen: Policy-to-circuit transpiler," in *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 1–5, IEEE, 2024

[1] The symbol * indicates that the authors equally contributed to the work.

- J. Ernstberger, **J. Lauinger**, F. Elsheimy, L. Zhou, S. Steinhorst, R. Canetti, A. Miller, A. Gervais, and D. Song, “Sok: Data sovereignty,” in *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*, (Los Alamitos, CA, USA), pp. 122–143, IEEE Computer Society, jul 2023
- J. **Lauinger**, J. Ernstberger, and S. Steinhorst, “Anonymous domain ownership,” in *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 1–3, IEEE, 2023
- A. Finkenzeller, A. Mathur, J. **Lauinger**, M. Hamad, and S. Steinhorst, “Simutack-an attack simulation framework for connected and autonomous vehicles,” in *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, pp. 1–7, IEEE, 2023
- J. **Lauinger**, M. Hamad, and S. Steinhorst, “Toward a multi-layer intrusion response system for connected vehicles,” in *2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall)*, pp. 1–2, IEEE, 2022
- M. Hamad, A. Finkenzeller, H. Liu, J. **Lauinger**, V. Prevelakis, and S. Steinhorst, “Seemqtt: Secure end-to-end mqtt-based communication for mobile iot systems using secret sharing and trust delegation,” *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3384–3406, 2022
- J. **Lauinger**, A. Finkenzeller, H. Lautebach, M. Hamad, and S. Steinhorst, “Attack data generation framework for autonomous vehicle sensors,” in *2022 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 128–131, IEEE, 2022
- M. Hamad, E. Regnath, J. **Lauinger**, V. Prevelakis, and S. Steinhorst, “Spps: secure policy-based publish/subscribe system for v2c communication,” in *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 529–534, IEEE, 2021
- J. **Lauinger**, J. Ernstberger, E. Regnath, M. Hamad, and S. Steinhorst, “A-poa: Anonymous proof of authorization for decentralized identity management,” in *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 1–9, IEEE, 2021
- A. Theodouli, K. Moschou, K. Votis, D. Tzovaras, J. **Lauinger**, and S. Steinhorst, “Towards a blockchain-based identity and trust management framework for the iov ecosystem,” in *2020 Global Internet of Things Summit (GIoTS)*, pp. 1–6, IEEE, 2020

RESEARCH & INDUSTRY INTERESTS

Zero-knowledge proof systems, secure data provenance, blockchain scaling protocols, data privacy, decentralized identity, multi-party computation, cloud security, certification systems, distributed systems, protocol and system design.