Felix Viktor Jedrzejewski

felix.jedrzejewski@gbth.se LinkedIn Profile
https://www.bth.se/eng/staff/felix-jedrzejewski-fje/

Employment History

2022 – Present **Ph.D. Student,** Blekinge Institute of Technology (BTH).

2018 – 2021 **Working Student in the Information Technology Security Research Group.** Corporate Technology, Siemens AG.

Education

2022 – Present **Ph.D. Student in Software Engineering, Blekinge Institute of Technology (BTH)** in Karlskrona, Sweden.
Thesis title: *Threat Modeling for Industrial Machine Learning Systems.*

2019 – 2021 **M.Sc. Information Systems, Technical University Munich (TUM)** in Munich, Germany.
Thesis title: *Privacy-Preserving Natural Language Processing: A Systematic Mapping Study*.

2017 – 2017 **Study Abroad, Johns Hopkins Whiting School of Engineering** in Baltimore, Maryland, USA.
Selected Courses: Critical Infrastructure Protection, Computer Forensics, Security Analytics, Practical Cryptographic Systems, WWW Security.

2014 – 2019 **B.Sc. Information Systems, Technical University Munich (TUM)** in Munich, Germany.
Thesis title: *Development of a Methodology for a structured Evaluation of Web Application Frameworks for Secure Software Development*.

Research Publications

Journal Articles

1. F. V. Jedrzejewski, L. Thode, J. Fischbach, T. Gorschek, D. Mendez, and N. Lavesson, "Adversarial machine learning in industry: A systematic literature review," *Available at SSRN 4737990*,

Conference Proceedings

1. F. V. Jedrzejewski, "Threat modeling of ml-intensive systems: Research proposal," in *Proceedings of the 3rd International Conference on AI Engineering — Software Engineering for AI*, 2024.
2. F. V. Jedrzejewski, D. Fucci, and O. Adamov, "Mlsmm: Machine learning security maturity model," in *The Second Workshop on New Frontiers in Adversarial Machine Learning*, 2023.
3. L. Watkins, J. Ramos, G. Snow, *et al.*, "Exploiting multi-vendor vulnerabilities as back-doors to counter the threat of rogue small unmanned aerial systems," in *Proceedings of the 1st ACM MobiHoc workshop on mobile IoT sensing, security, and privacy*, 2018, pp. 1–6.