**Present Address**
Berlin, Germany

# Anjo Vahldiek-Oberwagner

**Contact Info**
anjovahldiek@gmail.com
Phone: +49 173 154 88 46
https://vahldiek.github.io

## INTERESTS

Analyzing, designing, building, and evaluating the security, performance, and usability of hardware and software systems. My current research focuses on building secure systems including techniques protecting data confidentiality and integrity of sensitive data in-memory.

## EXPERIENCE

**Research Scientist at Intel Labs** April'19 – now
Intel Labs - Datacenter Security Group, Hillsboro, OR (2019-2022) → Berlin (starting July 2022)

**Research and develop security technologies for the datacenter by building prototypes and guiding technology transfers**

- Confidential Compute Cloud-native performance and usability improvements (Gramine Shielded Containers)
- LLMs/AI/ML in Confidential Computing improving security and privacy
- Memory isolation techniques improving security and performance for datacenter workloads
- Multiple open-source releases, PRs and projects (e.g., initial developer of Gramine Shielded Containers).
- Established 7 academic collaborations and transferred multiple technologies into Intel products and open-source projects (e.g., WAMR).
- Current Focus: Benchmarking and performance analysis of LLMs (i.e., Llama2/3) inside Intel's confidential compute TEEs. Root cause performance observations and improve performance. Build the foundation for a shielded private compound AI/LLM service inside TEEs.

**Adjunct Lecturer at TUM** July'22 – now
At Distributed & Operating Systems Chair

**Research Software Engineering Intern** Summer 2014
Microsoft Research, Redmond, WA

Research opportunities to overcome performance and flexibility issues with Trusted Platform Modules (TPM) using Intel's new Software Guard Extension (SGX). Build and evaluate a prototype implementation.

**Software Engineering Intern/Bachelor Thesis** 2006 - 2009
IBM, Boeblingen, Germany & Austin, Texas, USA

Analyzed, designed and implemented prototypes. Optimizing Informix Dynamic Servers (IDS), programming models for heterogeneous processor architectures.

**Ph.D. Candidate** co-advised by Peter Druschel & Deepak Garg 2010 – 2019
Max Planck Institute for Software Systems, Saarbruecken, Germany

**Ph.D. Candidate** mentored by Holger Hermanns 2009 – 2010
Saarland University, Graduate School, Saarbruecken, Germany

**Bachelor of Science** in Applied Computer Science 2006 – 2009
Baden-Württemberg Cooperative State University Stuttgart (DHBW Stuttgart) with IBM Germany
Thesis: "Distributed Complex Query Processing for Informix Dynamic Server"
GPA: 1.5 (scale 1.0 to 5.0), First Class, Top 10%

## SKILLS

C, Python, Operating Systems, Secure System Design, Distributed Systems, Storage Systems, Trusted Computing, SSD/Flash Memory, Linux, Memory Safety and Isolation

## Selected PUBLICATIONS

Complete list: Google Scholar
Top Venues: USENIX Security (4), EuroSys (3), ASPLOS(2), CCS (1), OSDI (1), IEEE S&P (1)

*Fortify Your Foundations: Practical Privacy and Security for Foundation Model Deployments In The Cloud*
Marcin Chrapek, **Anjo Vahldiek-Oberwagner**, Marcin Spoczynski, Scott Constable, Mona Vij, Torsten Hoefler
arXiv 2024

*Segue & ColorGuard: Optimizing SFI Performance and Scalability on Modern Architectures*
Shravan Narayan, Tal Garfinkel, Evan Johnson, Zachary Yedidia, Yingchen Wang, Andrew Brown, **Anjo Vahldiek-Oberwagner**, Michael LeMay, Wenyong Huang, Xin Wang, Mingqui Sun, Dean Tullsen, Deian Stefan
**To appear in ASPLOS 2025**

*Pegasus: Transparent and Unified Kernel-Bypass Networking for Fast Local and Remote Communication*
Dinglan Peng, Congyu Liu, Tapti Palit, **Anjo Vahldiek-Oberwagner**, Mona Vij, Pedro Fonseca
**To appear ACM EuroSys 2025**

*Hardware-Assisted Fault Isolation: Going Beyond the Limits of Software-Based Sandboxing*
Shravan Narayan, Tal Garfinkel, Mohammadkazem Taram, Joey Rudek, Daniel Moghimi, Evan Johnson, **Anjo**

**Vahldiek-Oberwagner**, Michael LeMay, Ravi Sahita, Dean Tullsen, Deian Stefan
**IEEE Micro Top Picks 2024 Volume 44, Number 4**

*Endokernel: A Thread Safe Monitor for Lightweight Subprocess Isolation*
Fangfei Yang, Bumjin Im, Weijie Huang, Kelly Kaoudis, **Anjo Vahldiek-Oberwagner**, Chia-Che Tsai, Nathan Dautenhahn
**USENIX Security 2024**

*Trusted Heterogeneous Disaggregated Architectures*
Atsushi Koshiba, Felix Gust, Julian Pritzi, **Anjo Vahldiek-Oberwagner**, Nuno Santos, Pramod Bhatotia
APSys Workshop 2023

*Going beyond the Limits of SFI: Flexible and Secure Hardware-Assisted In-Process Isolation with HFI*
Shravan Narayan, Tal Garfinkel, Mohammadkazem Taram, Joey Rudek, Evan Johnson, **Anjo Vahldiek-Oberwagner**, Michael LeMay, Ravi Sahita, Dean Tullsen, Deian Stefan
**ASPLOS 2023, Distinguished Paper Award**

*uSWITCH: Fast Kernel Context Isolation with Implicit Context Switches*
Dinglan Peng, Congyu Liu, Tapti Palit, Pedro Fonseca, **Anjo Vahldiek-Oberwagner**, Mona Vij
**IEEE Security & Privacy 2023**

*Segue & ColorGuard: Optimizing SFI Performance and Scalability on Modern x86*
Shravan Narayan, Tal Garfinkel, Evan Johnson, David Thien, Joey Rudek, Michael LeMay, **Anjo Vahldiek-Oberwagner,** Dean Tullsen, Deian Stefan
PLAS Workshop 2022

*MeSHwA: The case for a Memory-Safe Software and Hardware Architecture for Serverless Computing*
**Anjo Vahldiek-Oberwagner**, Mona Vij

WORDS Workshop 2022

*Cerberus: A Formal Approach to Secure and Efficient Enclave Memory Sharing*
Dayeol Lee, Kevin Cheang, Alexander Thomas, Catherine Lu, Pranav Gaddamadugu, **Anjo Vahldiek-Oberwagner**, Mona Vij, Dawn Song, Sanjit A Seshia, Krste Asanović
**ACM CCS 2022**

*Swivel: Hardening WebAssembly against Spectre*
Shravan Narayan, Craig Disselkoen, Daniel Moghimi, Sunjay Cauligi, Evan Johnson, Zhao Gang, **Anjo Vahldiek-Oberwagner**, Ravi Sahita, Hovav Shacham, Dean Tullsen, Deian Stefan
**USENIX Security 2021**

*Tutorial: Graphene: Confidential Computing for Unmodified Linux Applications*
**Anjo Vahldiek-Oberwagner**, Chia-Che Tsai, Dmitrii Kuvaiskii, Don Porter
IEEE Secure Development Conference (SecDev), 2020

*Privacy-Preserving Machine Learning in Untrusted Clouds Made Simple*
Dayeol Lee, Dmitrii Kuvaiskii, **Anjo Vahldiek-Oberwagner**, Mona Vij
arXiv 2020

*ERIM: Secure, Efficient In-process Isolation with Memory Protection Keys*
**Anjo Vahldiek-Oberwagner**, Eslam Elnikety, Nuno O. Duarte, Michael Sammler, Peter Druschel, Deepak Garg
**USENIX Security 2019**
**Distinguished Paper Award and Internet Defense Prize 2019**

*PESOS: Policy Enhanced Secure Object Store*
Robert Krahn, Bohdan Trach, **Anjo Vahldiek-Oberwagner**, Thomas Knauth, Pramod Bhatotia, Christof Fetzer
**ACM EuroSys 2018**

*Light-Weight Contexts: An OS Abstraction for Safety and Performance*
James Litton, **Anjo Vahldiek-Oberwagner**, Eslam Elnikety, Deepak Garg, Bobby Bhattacharjee, Peter Druschel
**USENIX OSDI 2016**

*Thoth: Comprehensive Policy Compliance in Data Retrieval Systems*
Eslam Elnikety, Aastha Mehta, **Anjo Vahldiek-Oberwagner**, Deepak Garg, Peter Druschel
**USENIX Security 2016**

*Guardat: Enforcing data policies at the storage layer*
**Anjo Vahldiek-Oberwagner**, Eslam Elnikety, Aastha Mehta, Peter Druschel, Deepak Garg, Rodrigo Rodrigues, Johannes Gehrke, Ansley Post
**ACM EuroSys 2015**

## Patents

Granted: 4 Applications: 9

US Patent App. 18/676,413 (2024): METHODS AND APPARATUS TO VERIFY THE INTEGRITY OF A MODEL
Scott Douglas Constable, Marcin Andrzej Chrapek, Marcin Spoczynski, Cory Cornelius, Mona Vij, **Anjo Lucas Vahldiek-Oberwagner**

US Patent App. 18/665,188 (2024): Artificial intelligence model accuracy validation
**Anjo Lucas Vahldiek-Oberwagner**, Marcin Andrzej Chrapek, Scott Constable

US Patent App. 17/853,087 (2023): Reducing instrumentation code bloat and performance overheads using a runtime call instruction
Michael LeMay, Dan Baum, Joseph Cihula, Joao Batista Correa Gomes Moreira, **Anjo Lucas Vahldiek-Oberwagner**, Scott Constable, Andreas Kleen, Konrad Lai, Henrique de Medeiros KAWAKAMI, David M Durham

US Patent App. 18 / 311,253 (2023): Method and apparatus for multi-dimensional attestation for a software application
Marcela S Melara, Bruno Vavala, Michael Steiner, Vincent Scarlata, **Anjo Lucas Vahldiek-Oberwagner**

US Patent 11,650,800 (2023): Attestation of operations by tool chains
Vincent Scarlata, Alpa Trivedi, Reshma Lal, Marcela S Melara, Michael Steiner, **Anjo Vahldiek-Oberwagner**

US Patent 12,013,954 (2024): Scalable cloning and replication for trusted execution environments
Ravi Sahita, Dror Caspi, Vedvyas Shanbhogue, Vincent Scarlata, **Anjo Lucas Vahldiek-Oberwagner**, Haidong Xia, Mona Vij

US Patent 12,019,562 (2024): Cryptographic computing including enhanced cryptographic addresses
Michael D LeMay, David M Durham, **Anjo Lucas Vahldiek-Oberwagner**, Anna Trikalinou

US Patent App. 17/561,676 (2022): Optimizing deployment and security of microservices
Paritosh Saxena, **Anjo Lucas Vahldiek-Oberwagner**, Mona Vij, Kshitij A Doshi, Carlos H Morales, Clair Bowman, Marcela S Melara, Michael Steiner

US Patent App. 17/314,349 (2021): TECHNOLOGY TO CONTROL SYSTEM CALL INVOCATIONS WITHIN A SINGLE ADDRESS SPACE
Michael Lemay, **Anjo Vahldiek-Oberwagner**

US Patent App. 17/131,716 (2021): Reducing latency of hardware trusted execution environments
**Anjo Lucas Vahldiek-Oberwagner**, Ravi L Sahita, Mona Vij, Rameshkumar Illikkal, Michael Steiner, Thomas Knauth, Dmitrii Kuvaiskii, Sudha Krishnakumar, Krystof C Zmudzinski, Vincent Scarlata, Francis McKeen

US Patent App. 17/131,684 (2021): Scalable attestation for trusted execution environments
**Anjo Lucas Vahldiek-Oberwagner**, Ravi L Sahita, Mona Vij, Dayeol Lee, Haidong Xia, Rameshkumar Illikkal, Samuel Ortiz, Kshitij Arun Doshi, Mourad Cherfaoui, Andrzej Kuriata, Teck Joo Goh

US Patent App. 17/131,751 (2021): Isolating memory within trusted execution environments
Ravi L Sahita, **Anjo Lucas Vahldiek-Oberwagner**, Teck Joo Goh, Rameshkmar Illikkal, Andrzej Kuriata, Vedvyas Shanbhogue, Mona Vij, Haidong Xia

US Patent 9,165,155 (2015): Protecting the integrity and privacy of data with storage leases
Peter Druschel, Rodrigo Rodrigues, Ansley Post, Johannes Gehrke, **Anjo Lucas Vahldiek**

## Honors & Awards

2024 Intel Hardware Security Academic Award 2024 Honorable Mention for HFI
2023 ASPLOS Distinguished Paper Award
2022 Selected as DARPA Riser 2022, Topic: "The Rise of Memory-Safe Languages: Building a Fast, Elastic, Secure Software & Hardware Architecture"
2021 Intel High-5 Patent Award
2021 Intel Labs Gordy Award Honorable Mention in "Excelence in Risk Taking" for our continued work on the Graphene Library OS (in collaboration with Dmitrii Kuvaiskii, Mona Vij, Sudha Krishnakumar, Isaku Yamahata)
2019 USENIX and Facebook Internet Defense Prize
2019 USENIX Security Distinguished Paper Award
2010-2016 Max Planck Society, PhD Scholarship
2009 Saarland University, Graduate School PhD Scholarship
2007 IBM International Internship Scholarship

## Program Committee & Review Service

USENIX Security'25 PC
ACM TOPS Associate Editor (since summer 2024)
EuroSys'25 PC
USENIX Security'24 PC & Research Ethics Committee
ACM Conference on Reproducibility and Replicability'24 PC

ACM Conference on Reproducibility and Replicability’23 PC
USENIX Security’23 PC
USENIX Security’22 PC
USENIX Security’21 PC
Middleware’20 Doctoral Workshop PC
EuroSys’20 ShadowPC
SOCC’19 Poster PC
External reviewer EuroSys’18
External reviewer HotOS’17
External reviewer OSDI’16

**Artifact Evaluation Service**

USENIX Security’24 Artifact Evaluation co-chair
USENIX Security’23 Artifact Evaluation co-chair
EuroSys’22 Artifact Evaluation co-chair
SuperComputing’21 Artifact Evaluation co-chair
OSDI’20 Artifact Evaluation co-chair
USENIX Security’20 Artifact Evaluation Committee
SOSP’19 Artifact Evaluation Committee

**Organization Service & Activities**

Steering committee of ACM Conference on Reproducibility and Replicability
Steering committee of NSF Repeto Project
EuroSys’21 registration and finance co-chair
Co-Develop WelcomeHelp.de Refugee Volunteer Tool
Student Admission Volunteer MPI-SWS
General Student Meeting Coordinator MPI-SWS