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
Datacenter Security Group, Hillsboro, OR (2019-2022) and Berlin (starting July 2022)

Research and develop security technologies for the datacenter by building prototypes, guiding technology transfers, and advising corporate strategy

- Led development of Gramine Shielded Containers to enable cloud-native workloads in TEEs
- Led performance benchmarking of LLMs in TEEs, 2 CPU performance issues solved
- Led 2 corporate wide technology and strategic teams on memory-safe languages (2022) and in-process (2023)
- Led development of in-process isolation technique and productization efforts with customers
- Multiple open-source releases, PRs and projects (e.g., Gramine Shielded Containers)
- Established 10 academic collaborations and transferred multiple technologies into Intel products and open-source projects (e.g., WAMR)
- Recent Focus: Benchmarking and performance analysis of LLMs (i.e., Llama2/3) inside Intel's confidential compute TEEs. Build the foundation for a private compound AI/LLM service.

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 prototype implementations.

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.

Education

Ph.D. Candidate co-advised by Peter Druschel & Deepak Garg 2010 – 2019
Max Planck Institute for Software Systems & Saarland University, 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, Confidential Computing, SSD/Flash Memory, Linux, Memory Safety and Isolation, LLMs, Secure AI

Selected PUBLICATIONS

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

Lessons Learned from Five Years of Artifact Evaluations at EuroSys
Daniele Cono D'Elia, Thaleia Dimitra Doudali, Cristiano Giuffrida, Miguel Matos, Mathias Payer, Solal Pirelli, Georgios Portokalidis, Valerio Schiavoni, Salvatore Signorello, **Anjo Vahldiek-Oberwagner**
ACM REP

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
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
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

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 (S&P) 2023

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

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

Selected Patents (5 granted, 8 filed)

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 12,113,902 (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 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 Corporate Research Council Mentor of the Month December 2024
2024 HFI selected into IEEE Micro Top Picks 2024
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 "Excellence 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

Phd. Thesis Comittee

Marcin Chrapek (ETH Zurich) – expected 2026
Prateek Sahu (UT Austin) – expected 2025
Merve Gülmez (KU Leuven) – expected 2025
Claudio Correia (Universidade de Lisboa) – 2024
Atri Bhattacharyya (EPFL) – 2024
Dayeol Lee (UC Berkeley) – 2022

Supervised Internships

Kevin Morio (CISPA) – 2024
Supraja Sridhara (ETH Zurich) – 2024
Fangfei Yang (Rice University) – 2022
Carlos Segarra (Imperial College London) – 2022
Dayoel Lee (UC Berkeley) – 2021

Program Committee Chair & Area Chair

EuroS&P 2026 Area chair for System Security
Systex 2025 PC co-chair

Program Committee & Review Service

EuroSys: 2025, 2026
USENIX Security: 2021, 2022, 2023, 2024, 2025
ACM Conference on Reproducibility and Replicability: 2023, 2024, 2025
ACM TOPS Associate Editor: 2024, 2025
Middleware Doctoral Workshop PC: 2020
EuroSys ShadowPC: 2020
SOCC Poster PC: 2019
External reviewer: EuroSys'18, HotOS'17, 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

Founding maintainer of sysartifacts.github.io and secartifacts.github.io
Steering committee of ACM Conference on Reproducibility and Replicability
Steering committee of NSF Repeto Project
EuroSys'21 registration and finance co-chair