Present Address
Berlin, Germany

Anjo Vahldiek-Oberwagner

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

INTERESTS

I'm interested in tackling hard problems by analyzing, designing, building, and evaluating software systems. My current research focuses on building secure systems including techniques protecting data confidentiality and integrity of sensitive data at rest, in-flight or in-memory.

INDUSTRIAL EXPERIENCE

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

Research Scientist at Intel Labs April'19 – now
Intel Labs, Hillsboro, OR → Now remote from Berlin
Research and improve security technologies. Build prototypes and guide technology transfers.
Current focus: Building secure cloud-native prototypes, and memory protection techniques.

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.

EDUCATION

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

ACADEMIC HIGHLIGHTS

ERIM: Secure, Efficient in-process isolation with Protection keys (MPK) [USENIX Security'19]
Isolating sensitive state and data can increase the security and robustness of many applications. Examples include protecting cryptographic keys against exploits like OpenSSL's Heartbleed bug or protecting a language runtime from native libraries written in unsafe languages. ERIM, a novel technique that provides hardware-enforced isolation with low overhead on x86 CPUs, even at high switching rates.

Guardat: Enforcing data policies at the storage layer [EuroSys'15]
In today's systems, policies protecting stored data and mechanisms for their enforcement are spread across many software components, increasing the risk of violation due to bugs, vulnerabilities and misconfigurations. Using Guardat, users, developers and administrators specify file protection policies declaratively, concisely and separate from code, and Guardat enforces these policies by mediating I/O in the storage layer.

PUBLICATIONS

Complete list: Google Scholar
Top Venues (count since 2015): USENIX Security (3), EuroSys (2), ACM CCS (1), OSDI (1), IEEE S&P (1)

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

Expanding the Scope of Artifact Evaluation at HPC Conferences: Experience of SC21
Tanu Malik, **Anjo Vahldiek-Oberwagner**, Ivo Jimenez, Carlos Maltzahn
P-RECS Workshop 2022

The Endokernel: Fast, Secure, and Programmable Subprocess Virtualization
Bumjin Im, Fangfei Yang, Chia-Che Tasi, Michael LeMay, **Anjo Vahldiek-Oberwagner**, Nathan Dautenhahn
arXiv 2021

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

Techniques to Protect Confidentiality and Integrity of Persistent and In-Memory Data
Anjo Vahldiek-Oberwagner
PhD Thesis 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

Protecting Data Integrity with Storage Leases
Anjo Vahldiek, Eslam Elnikety, Ansley Post, Peter Druschel, Rodrigo Rodrigues
Technical Report 2011-08, MPI-SWS, 2011 & **granted patent**

A Verified Dependable Wireless Safety Critical Hard Real-Time Design
Hernan Baro Graf, Holger Hermanns, Juhi Kulshrestha, Jens Peter, **Anjo Vahldiek**, Aravind Vasudevan
IEEE WoWMoM 2011

Evaluation of an Optimization for Object Tracking – Feedback-Based Head-Tracking
Anjo Vahldiek, Ansgar Schneider, Stefan Schubert, Dirk Reichard
Fifth Annual Meeting on Information Technology and Computer Science of the Baden-Wuerttemberg Cooperative State University, 2009

Patents

Granted: 1 Applications: 8

US Patent App. 17/710,723 (2022): 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 App. 17/481,405 (2022): Cryptographic computing including enhanced cryptographic addresses
Michael D LeMay, David M Durham, **Anjo Lucas Vahldiek-Oberwagner**, Anna Trikalinou

US Patent App. 17/133,880 (2022): Attestation of operations by tool chains
Vincent Scarlata, Alpa Trivedi, Reshma Lal, Marcela S Melara, Michael Steiner, **Anjo Vahldiek-Oberwagner**

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): Scalabe 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**

Talks

MeSHwA: The case for a Memory-Safe Software and Hardware Architecture for Serverless Computing
Anjo Vahldiek-Oberwagner
WORDS Workshop 2022

Breaking with traditional OS Abstractions
Anjo Vahldiek-Oberwagner
Guest Lecture for Operating System class at IIT Kharagpur in 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

Automatically Securing Linux Application Containers in Untrusted Clouds
Anjo Vahldiek-Oberwagner, Dmitrii Kuvaiskii
Linux Security Summit, Refereed Presentation, 2020

ERIM: Secure, Efficient In-process Isolation with Memory Protection Keys
Anjo Vahldiek-Oberwagner
USENIX Security, 2019

Enforcing Confidentiality and Integrity Policies over untrusted Applications
Anjo Vahldiek-Oberwagner
Intel Labs, 2016
Bell Labs, 2016

Guardat: Enforcing data policies at the Storage layer
Anjo Vahldiek-Oberwagner
EuroSys, 2015
Microsoft Research, 2014

Trusted Storage
Anjo Vahldiek-Oberwagner
USENIX FAST Conference Work in Progress, 2012

WiP/Posters

The Rise of Memory-Safe Languages: Building a Fast, Elastic, Secure Software & Hardware Architecture
Anjo Vahldiek-Oberwagner
DARPA Forward Conference as DARPA Riser 2022

Thoth: Efficiently enforcing data confidentiality and integrity in large-scale distributed data processing systems
Eslam Elnikety, **Anjo Vahldiek**, Aastha Mehta, Deepak Garg, Peter Druschel
ACM SOSP'13 Work in progress

Trusted Storage
Anjo Vahldiek, Eslam Elnikety, Ansley Post, Peter Druschel, Deepak Garg, Johannes Gehrke, Rodrigo Rodrigues
Usenix FAST'12 Work in progress

Honors & Awards	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	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'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