Anjo Vahldiek-Oberwagner

Present Address
Portland, Oregon
United States of America

Contact Info
anjovahldiek@gmail.com
Phone: +1 503 4530 673
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.

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.

INDUSTRIAL EXPERIENCE

Research Scientist at Intel Labs April'19 – now
Intel Labs, Hillsboro, OR

Research and improve security technologies. Build prototypes and provide guidance to their technology transfer. Current focus lies in building secure, accountable machine learning training and Function-as-a-Service 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. Mentor: Ronald Aigner (Principal Research Engineer)

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

Analyzed, designed and implemented prototypes. From optimizing distributed queries in Informix Dynamic Servers (IDS) to providing new programming models for heterogeneous processor architectures like the Cell/BE.

Publications

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

Talks

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
USENIX Security, 2019

Enforcing Confidentiality and Integrity Policies over untrusted Applications
Intel Labs, 2016
Bell Labs, 2016

Guardat: Enforcing data policies at the Storage layer
EuroSys, 2015
Microsoft Research, 2014

Trusted Storage
Fast WiP, 2012

WiP/Posters

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

Teaching

TA for Distributed Systems	Winter 2014
TA for Operating Systems	Summer 2011

Honors & Awards

USENIX and Facebook Internet Defense Prize	2019
USENIX Security Distinguished Paper Award	2019
Max Planck Society, PhD Scholarship	2010 - 2016
Saarland University, Graduate School PhD Scholarship	2009
IBM International Internship Scholarship	2007

Program Committee & Review Service

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

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

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