JOHANNES SPÄTH, PhD

(+49) 176 21 327 509 ◇ joh.spaeth@gmail.com ◇ johspaeth.de
Barer Str. 54 ◇ 80799 Munich

Computer scientist and engineer with 12 years of experience spanning academic research, startup founding, and technical leadership. Specializes in program analysis, formal verification, and software security, with a track record of translating deep theoretical work into production tools and commercial products.

WORK EXPERIENCE (12 YEARS)

Certora Ltd August 2023 - July 2026
R&D Director (since December 2023, initially hired as Senior Software Engineer) *Munich, Germany*

Certora provides security audits and automated formal verification for web3 protocols. With the "Prover", Certora builds a product that uses SMT solvers to mathematically verify the implementation of smart contracts.

Responsibilities & Tasks

- Leading different teams of compiler and software engineers to enhance the Prover across different blockchain ecosystems (Ethereum, Stellar, Solana)
- Contributed to the Prover and to Certora's specification language (CVL and CVLR): added support for strong invariant logic, lifted LLVM debug information to present counterexamples in IDEs, implemented a program interpreter over the IR, and worked on LLM-based spec generation
- Delivered hands-on Certora Prover workshops at TrustX 2023 (Istanbul) and Meridian 2024 (London), introducing developers to formal verification techniques for smart contract security

CodeShield GmbH November 2019 - June 2023
CEO & Co-Founder *Paderborn / Munich, Germany*

CodeShield is a Software-as-a-Service that detects and fixes cloud security vulnerabilities (Gartner terms: CIEM, CNAPP, CSPM).

Responsibilities & Tasks

- Acquiring and implementing proof-of-concepts with national and international clients
- Securing funding to build and grow the team
- Leading customer research, defining the product vision, iterating on MVP: Discover IAM permission misconfigurations and demonstrate exploitable attack vectors (IAM privilege escalations)

Fraunhofer IEM - Institute for Mechatronic Systems Design March 2017 - October 2019
Senior Expert & Research Associate *Paderborn, Germany*

The department of Software Engineering and IT Security at Fraunhofer IEM develops and researches on methods and tools for secure development, maintenance, and operation of software-intensive systems.

Responsibilities & Tasks

- Research on efficient and precise program analysis with focus on security (pointer and taint analyses)
- Development of the IDE plugin Eclipse CogniCrypt: a spell checker for developers detecting insecure usages of cryptographic APIs, presented at EclipseCon Europe 2018 and heise devSec 2019
- Integration of static code analyses with industry partners (SAST & SCA for DevOps)
- Acquisition of industry and research projects with volume of more than 1M EUR

Oracle August 2016 - January 2017
Research Intern *Brisbane, Australia*

Oracle Labs Brisbane is one of Oracle's eight research centers. The team in Brisbane develops program analysis technologies for internal use (Oracle Parfait).

Responsibilities & Tasks

- Research stay to work on existing data flow and code analyses solution
- Prototyping and implementing concepts for efficient program analysis based on soufflé (Datalog-based program analysis)
- C++-implementation for points-to summaries on top of soufflé

Fraunhofer SIT - Institute for Secure Information Technology March 2014 - July 2016
Research Associate *Darmstadt, Germany*

Responsibilities & Tasks

- Researching and prototyping program and data-flow analyses (pointer and taint analyses)
- Security analysis of the source code of TrueCrypt using Coverity Scan and Fortify, commissioned by the German Federal Office for Information Security (BSI)
- Security & pen testing of web applications using OWASP ZAP & Wireshark

ACADEMIC DEGREES

PhD in Computer Science (Dr. rer. nat.) *January 2019*
Paderborn University
Dissertation: *Synchronized Pushdown Systems for Pointer and Data-Flow Analysis*
Grade: *summa cum laude (received 3 awards)*

Master of Science in Mathematics with Specialisation in Computer Science *September 2013*
Technical University of Darmstadt
Grade: 1.6

Bachelor of Science in Mathematics *March 2011*
Johannes Gutenberg University of Mainz
Grade: 1.6

TECHNOLOGY SKILLS

Scale: ●●●●● *Expert* ●●●●○ *Advanced* ●●●○○ *Proficient* ●●○○○ *Familiar*

Programming Languages		**PL & FV Tooling**	
Kotlin / Java	●●●●●	Soot	●●●●●
TypeScript / JavaScript	●●●●○	WALA	●●●●●
Rust	●●●●○	SMT Solving	●●●●○
Python	●●●○○	Lean	●●○○○
C/C++	●●○○○	LLVM	●●○○○

SPOKEN LANGUAGES

- German - native
- English - fluent
- French - basic

SELECTED PUBLICATIONS & PATENTS

- *CrySL: An Extensible Approach to Validating the Correct Usage of Cryptographic APIs.*
  Stefan Krüger, Johannes Späth, Karim Ali, Eric Bodden, Mira Mezini. *In Transactions on Software Engineering (TSE), 2019.*
- *Context-, Flow- and Field- Sensitive Data-Flow Analysis using Synchronized Pushdown Systems.*
  Johannes Späth, Karim Ali, Eric Bodden. *In Symposium on Principles of Programming Languages (POPL), 2019.*
- *Boomerang: Demand-Driven Flow- and Context-Sensitive Pointer Analysis for Java.*
  Johannes Späth, Lisa Nguyen Quang Do, Karim Ali, Eric Bodden. *In European Conference on Object-Oriented Programming (ECOOP), 2016.*
- *Security Analysis of TrueCrypt*
  Mauro Baluda, Andreas Fuchs, Philipp Holzinger, Lisa Nguyen, Lotfi ben Othmane, Andreas Poller, Jürgen Repp, Johannes Späth, Jan Steffan, Stefan Triller, Eric Bodden. *Federal Office for Information Security, 2015.*
- *Modular Points-To Analysis. (Patent, Publication Number: 20190065180)*
  Johannes Späth, Francois Gauthier, Padmanabhan Krishnan. *Oracle International Corporation, 2017.*

AWARDS

- *Fraunhofer ICT Dissertation Award 2022*
- *Award by the Presidium of the University of Paderborn (Excellent Dissertation 2019)*
- *Ernst Denert Software-Engineering Award 2019*
- *Distinguished Paper Award (POPL 2019)*
- *Artifact Evaluation Award (POPL 2019, ECOOP 2016)*