Harshavardhan Unnibhavi

✉ harshavardhan.unnibhavi@tum.de
harshanavkis.github.io

Research Interests

I am broadly interested in systems research, with an emphasis on confidential computing, operating systems and emerging hardware architectures. The central theme of my current work is to employ a hardware-software co-design approach to develop secure systems that scale well and are resilient to failures. I am looking for internships during the summer of 2025 and am flexible with starting dates and durations.

Education

2021–Present **Ph.D.**, *Technical University of Munich*, Munich, Germany.
- Computer Science and Engineering
- Expected graduation date: December 2025
- Advisor: Prof. Pramod Bhatotia

2020–2021 **Master of Science by Research**, *The University of Edinburgh*, Edinburgh, UK.
- Computer Science
- Advisor: Prof. Pramod Bhatotia, Prof. Antonio Barbalace

2015–2019 **Bachelor of Technology**, *Indian Institute of Technology (IIT) Dhanbad*, Dhanbad, India.
- Electronics and Communication Engineering

Publications

Harshavardhan Unnibhavi, Julian Pritzi, Nils Asmussen, Carsten Weinhold, Michael Roitzsch, Nuno Santos, Pramod Bhatotia. Policy-Compliant Trusted Hardware-OS Acceleration with IronShield **(Under Submission)**

USENIX ATC'24 Jiyang Chen, **Harshavardhan Unnibhavi**, Atsushi Koshiba, Pramod Bhatotia. vFPIO: A Virtual I/O Abstraction for FPGA-accelerated I/O Devices. In Proceedings of the 2024 USENIX Annual Technical Conference.

SIGMOD'22 **Harshavardhan Unnibhavi**, David Cerdeira, Antonio Barbalace, Nuno Santos and Pramod Bhatotia. Secure and Policy-Compliant Query Processing on Heterogeneous Computational Storage Architectures. In Proceedings of the 2022 International Conference on Management of Data.

EuroSys'22 Jörg Thalheim, Peter Okelmann, **Harshavardhan Unnibhavi**, Redha Gouicem and Pramod Bhatotia. VMSH: Hypervisor-agnostic Guest Overlays for VMs. In Proceedings of the Seventeenth European Conference on Computer Systems (EuroSys).

EuroSys'21 Jörg Thalheim, **Harshavardhan Unnibhavi**, Christian Priebe, Pramod Bhatotia, and Peter Pietzuch. Rkt-io: a direct I/O stack for shielded execution. In Proceedings of the Sixteenth European Conference on Computer Systems (EuroSys).

Experience

2021–Present **Research Assistant**, *Technical University of Munich*, Munich, Germany.
- Mentor: Prof. Pramod Bhatotia

2024 **Research Intern**, *Intel Labs*, Munich, Germany.
- Mentor: Dr. Dmitrii Kuvaiskii, Mona Vij

2021 **Intern**, *QEMU*, Google Summer of Code (GSoC), Remote.
- Mentor: Stefano Garzarella, Fabiano Fidêncio

2019 **Research Assistant**, *Indian Institute of Science*, Bengaluru, India.
- Mentor: Prof. Yogesh Simmhan

2018 **Research Assistant**, *Simon Fraser University*, Burnaby, Canada.
- Mentor: Prof. Ivan V. Bajic

Talks

2024 **vFPIO: A Virtual I/O Abstraction for FPGA-accelerated I/O Devices**, *ATC '24*.

2022 **IronSafe: A Secure and Policy-Compliant Query Processing Architecture**, *SIGMOD '22*.

2022 **IronSafe: A Secure and Policy-Compliant Query Processing Architecture**, *MSR Cambridge*.
- Host: Dr. Kapil Vaswani

2021 **Development of a vhost-user-vsock application**, *Redhat*.
- Host: Stefano Garzarella

Research Experience

2024–Present **Confidential Disaggregated Acceleration**, TU Munich.
We are designing a HW/OS co-designed system to enable confidential access to accelerator devices in a physically disaggregated datacenter architecture without modifications to existing software stacks and hardware devices.

2024 **Cloud deployment of Gramine-TDX**, Intel Labs.
In this project, we designed a framework to enable applications (parent VMs) to offload security-sensitive tasks to confidential VMs running Gramine-TDX. We explored ways to provide access to I/O within the confidential VM over a minimal communication interface with the parent VM.

2023 **Virtual I/O Abstractions for FPGA-accelerated I/O**, TU Munich.
In this project, we are desiged an FPGA hardware shell that abstracts away the heterogeneity amongst the IO devices on an FPGA by providing simple and efficient to use abstractions and interfaces. This allows developers to concentrate solely on their acceleration logic by offloading the handling of IO devices to our shell.

2022–Present **Hardware/OS Co-design for Trusted Acceleration**, TU Munich.
We are designing a layered system stack that enables applications to securely use accelerators for their computations and obtain proofs of the same. The stack consists of programming libraries and interfaces, and an OS kernel that is co-designed with trusted hardware extensions.

2021–2022 **Shells for lightweight VMs**, TU Munich.
This project enables one to attach to and run services and tools on a virtual machine at runtime. This enables the VM to be as lightweight as possible while providing the ability to extend its functionality at runtime.

2020–2021 **Secure and policy compliant query processing on heterogeneous architectures**, TU Munich.
This project presents IronSafe, which allows applications to offload query processing operations to computational storage devices in a secure manner and obtain proofs of the same. We explored ways to extend the trust domain from the heterogeneous host to a storage device.

2020–2021 **Direct I/O stacks for shielded execution**, University of Edinburgh.
In this project, we designed a direct IO stack atop a library OS to allow applications to safely access IO devices from within a TEE. We explored ways to reduce the attack surface by minimizing interactions with the host OS while maintaining full POSIX compatibility.

Awards and Honors

2022 EuroSys'22 Best Artifact Award (Honorable Mention)

2018 Mitacs Globalink Fellowship

2015 KVPY Fellowship

2013 NTSE Fellowship

Teaching

2023 Introduction to Software Engineering

2023 Cloud Software Engineering

2022 Cloud Systems Engineering

2021 Practical lab: Swiss-knife for Computer System Systems

2021 Practical lab: Advanced Systems Programming in C/Rust

Research Advising

PhD

2024-Present Teofil Bodea: Secure on-device LLM inference

2023-Present Jiyang Chen: FPGA-accelerated I/O

Master's

2023 Julian Pritzi: Securing Hardware Communication using Encryption and Attestation

Undergraduate

2023 Jonas Zöschg: End-to-End On-Chip Encryption to Prevent Physical Attacks

2022 Julian Pritzi: An in-hardware cycle-accurate benchmarking tool for security critical operations

Technical Skills

Areas Operating Systems, Virtualization, Computer Architecture, Confidential Computing

Languages Verilog, Rust, C, Python, C++

Tools Vivado, Vivado HLS, Vitis, QEMU, KVM, gem5

References

Prof. Pramod Bhatotia,
TU Munich,
pramod.bhatotia@in.tum.de.

Prof. Antonio Barbalace,
The University of Edinburgh,
antonio.barbalace@ed.ac.uk.

Prof. Nuno Santos,
INESC-ID Lisbon,
nuno.m.santos@tecnico.ulisboa.pt.