Reshabh K Sharma

reshabh@cs.washington.edu · +1 (206)480-7245 · github/reSHARMA · linkedin/reshabh

Research Interests

Safety and security vulnerability mitigation, Program analysis, Compilers and secure compilation.

Education

PhD Computer Science and Engineering
Paul G. Allen School of Computer Science & Engineering
University of Washington, Seattle, WA
Advisor: Professor Dan Grossman
Sep 2021 - Present

B.Tech Computer Science and Engineering
National Institute of Technology Patna (NIT-P), Patna, India
Major Project at GRC Lab, IIT Bombay
Aug 2015 - May 2019

Experience

Paul G. Allen School of Computer Science & Engineering
Research Assistant
Advisor: Professor Dan Grossman
Sep 2024 - Present

- Secure compilation for hardware vulnerability mitigation.
- Side channel defense for prefetcher-based attacks on Apple M-series processors.
- Permission system for LLM-agent frameworks.

Straiker Inc.
Student Researcher
Advisor: Vinay Pidathala and Shreenath Kurupati
Sep 2024 - Present

- Discovery and implementation of attacks for LLM-based systems.

Microsoft Research
Research Intern
Advisor: Ben Zorn, Peli de Halleux, Markus Kuppe
June 2024 - Sep 2024

- Software engineering for prompts
- SIGPLAN Blog Post about our work Prompts are Programs.

Paul G. Allen School of Computer Science & Engineering
Research Assistant
Advisor: Professor Dan Grossman
June 2023 - June 2024
- Secure compilation for hardware vulnerability mitigation.
- Developing abstraction for efficiently enforcing safety and security properties for different domains like XR and LLM prompting.

Paul G. Allen School of Computer Science & Engineering
Research Assistant
Advisor: Professor Michael B. Taylor
Sep 2021 - June 2022
- PL for improving the development experience of hardware developers.
- Accelerating AI workloads by introducing instructions optimized for better hardware utilization of manycore architecture.

AMD Inc.
GPU Compiler Engineer
Aug 2019 - Sep 2021
- ROCm compiler and AMDGPU LLVM backend.
- Working on memory safety of heterogeneous programs.
- Extending LLVM Sanitizers to heterogeneous situations such as OpenCL and HIP.
- Driving the compiler effort from design perspective.
- Lead multiple RFCs to the LLVM community and contributed to the design of the instrumentations.

FOSSi - The Free and Open Source Silicon Foundation
Google Summer of Code intern'19
Advisor: Professor Michael B. Taylor
June 2019 - Aug 2019
- Implemented compiler support for the generic address space.
- Supported 64-bit pointers in RV32 for a RISCV based GPGPU.

GRC Lab, IIT Bombay
Research Assistant
Advisor: Professor Uday Khedker
Dec 2018 - Apr 2019
- Static virtual function call resolution in C++ using Demand-driven Alias analysis in LLVM.
- Focused on the reduction of size of callee set to boost inter-procedural analysis.
- Designed an abstraction from scratch to implement dataflow equations over LLVM IR.

LLVM - The LLVM Foundation

Google Summer of Code intern'18
Advisor: Sylvestre Ledru
Apr 2018 - Aug 2018

- Integrated libcxx* and OpenMP into llvm-toolchain.

Publications

1. **Reshabh K Sharma**, Vinayak Gupta, Dan Grossman. *Defending Language Models Against Image-Based Prompt Attacks via User-Provided Specifications.* Accepted to appear at SAGAI Workshop at IEEE S&P 2024.
2. Michael Flanders, **Reshabh K Sharma**, Alexandra E. Michael, Dan Grossman, David Kohlbrenner. *Avoiding Instruction-Centric Microarchitectural Timing Channels Via Binary-Code Transformations.* Accepted to appear at ASPLOS 2024.

Under Submission

1. **Reshabh K Sharma**, Dan Grossman, David Kohlbrenner. *Splitting Secrets: Compiler-Based Defense Against Content-Based Prefetcher Attacks*
2. **Reshabh K Sharma**, Vinayak Gupta, Dan Grossman. *SPML: A DSL for Defending Language Models Against Prompt Attacks.*

Selected Talks

1. **R. Sharma.** *Integration of OpenMP and libc++ packages into llvm-toolchain.* (2018)
   Poster for the 11th annual US LLVM Developer Meeting, San Jose, CA.
   Featured in The LLVM Blog and LLVM Weekly.

2. **R. Sharma.** *Lowering tale: Supporting 64 bit pointers in RISCV 32 bit LLVM backend.* (2019)
   Lightning talk and poster accepted for the 12th annual US LLVM Developer Meeting, San Jose, CA.
   Featured in the FOSSi blog.

3. **R. Sharma.** *Finding the cracks between the analysis.* (2021)
   Talk accepted for the LLVM Performance Workshop at CGO, Virtual.

Teaching Experience

1. **CSE331: Software Design and Implementation** (Teaching Assistant)
   Paul G. Allen School of Computer Science & Engineering, University of Washington

Summer 2022

2. **CSE548: Computer Systems Architecture** (Teaching Assistant)
   Paul G. Allen School of Computer Science & Engineering, University of Washington
   Autumn 2022
3. **CSE403: Software Engineering** (Teaching Assistant)
   Paul G. Allen School of Computer Science & Engineering, University of Washington
   Winter 2023
4. **CSE403: Software Engineering** (Teaching Assistant)
   Paul G. Allen School of Computer Science & Engineering, University of Washington
   Spring 2023

Service

ICFP'23
Student Volunteer

ACM SIGPLAN-M
Operations team member
July 2021 - Present

LLVM Social - Bangalore
Founder, Co-organizer
Nov 2019 - 2022

References

Dan Grossman (Doctoral Advisor)
Professor
Paul G. Allen School of Computer Science and Engineering
University of Washington
Website: https://homes.cs.washington.edu/ djg
Email: djg@cs.washington.edu