CHINMAY DESHPANDE

CONTACT INFORMATION

Github	chinmaydd	**Website**	https://chinmaydd.in
LinkedIn	chinmaydd	**Email**	chinmay1dd@gmail.com

ABOUT ME

I am broadly interested in the areas of compilers, software systems and security. I enjoy working on problems relating to low-level software development, reverse engineering, program (and binary) analysis and code performance. These days, I am intrigued by challenges and tradeoffs further down the stack, such as in hardware design.

EDUCATION

University of California Irvine *2019 - 2024*
Ph.D. in Computer Science GPA: 3.98/4.0
Dissertation: Practical Recompilation of Multithreaded Binaries

National Institute of Technology Karnataka, Surathkal *2013 - 2017*
B.Tech in Information Technology GPA: 8.87/10
Thesis: Optimizing Search Strategies in Binary Symbolic Execution

PUBLICATIONS

- **Chinmay Deshpande**, Fabian Parzefall, Felicitas Hetzelt and Michael Franz. Polynima: Practical Hybrid Recompilation for Multithreaded Binaries. EuroSys 2024. (Acceptance: 14.6%)
- Fabian Parzefall, **Chinmay Deshpande**, Felicitas Hetzelt and Michael Franz. What you trace is what you get: dynamic stack-layout recovery for binary recompilation. ASPLOS 2024. (Acceptance: 20%)
- **Chinmay Deshpande**, David Gens, and Michael Franz. StackBERT: Machine Learning Assisted Static Stack Frame Size Recovery on Stripped and Optimized Binaries. AISec @ ACM CCS 2021. (Acceptance: 21%)

EXPERIENCE

AMD Member of Technical Staff
ML Compilers and Languages Team *Fall '24 - Present*

- I currently work on the LLVM compiler backend that targets AMD GPUs, as part of the ROCm stack - with a focus on compute workloads on Windows machines.

Secure Systems and Software Lab, UC Irvine Research Assistant
Advisor: Prof. Michael Franz *2019 - 2024*

- Primarily worked on BinRec, a framework for the lifting and recompilation of x86/x64 binaries using LLVM IR. The project spans around 30 KLOC of C++ and is undisputedly (as of 2024) the most performant and robust recompiler out there.
- We achieved several goals in the context of this project: compatibility for multithreaded binaries, refining generated IR to move away from the "emulator" model, incremental lifting and cross-ISA binary translation. Towards the end, I was investigating fundamental security and correctness issues introduced by the recompilation process and how we can tackle them.

- I also contributed to MCA Daemon (MCAD), a framework that builds on top of llvm-mca and enables precise timing analysis of entire binary programs.

Vuln. Discovery and Mitigations Research, Qualcomm (QPSI) Engineering Intern
Mentor: Dr. Nilo Redini *Summer '23*

- Worked on applying symbolic taint analysis to find memory corruption vulnerabilities in kernel-mode driver binaries. The core challenge was to track interesting taint flow from unverified sources.
- Found and reported multiple bugs in critical QC software. Implemented improvements to the underlying engine that include precise handling of global variables, and identifying struct-based object overflows.

Automated Reasoning Group, Amazon Applied Scientist Intern
Mentor: Dr. Daniel Schwartz-Narbonne *Summer '21*

- Worked on a verification-friendly vector stub for the Rust Standard Library in the context of the Kani Verifier project - which performs formal verification of Rust programs.
- Project involved research and implementation of a host of vector abstractions of varying granularity to demonstrate significant improvements in proof performance and scalability.

Binary Ninja, Vector35 Intern
Mentor: Peter LaFosse *Summer '20*

- Implemented User-informed dataflow (UIDF), a feature which allows users to inform values to identified variables at the Medium-level IL (MLIL) layer. UIDF seeds the analysis with provided variable values and enables constant propagation, dead-code elimination based on the resulting dataflow.
- Was involved in the ideation, design and development of the feature - including core algorithms, API and the user-interface. Also worked on general bug-fixes and product improvement.

rune/radeco, radare2 Open-source Contributor
Mentor: Anton Kochkov *2016 - 2018*

- Implemented an Explorer module for a binary symbolic execution engine, to allow pre-defined choices at program points in lifted IR. Designed a new memory-module backend to support single-byte symbolic memory accesses. Also developed arch-rs, a library that provides abstractions for low-level architecture information.
- Mentored radeco, a decompiler project, which involved implementing control-flow restructuring and IR to AST translation for C-like pseudocode output as a part of GSoC.

McAfee Software Development Engineer
Windows Sandboxing (ATD) *2017 - 2019*

- Conducted research on binary sandboxing (user-mode hooking, process memory analysis, evasion techniques, etc.) and reverse engineering of Windows malware to improve their replication and detection.
- Worked on improving detection of script-based malware found embedded across environments such as WScript and PDFs using emulation. Also conducted attack-surface research for PDFs to develop a "prefilter" module, so as to quickly identify benign documents.

SKILLS

· **Languages**	C, C++, Python, Rust, asm: x86/64, ARM, AMDGCN
· **Libraries/Software**	LLVM, IDA Pro, gdb, WinDBG, Z3, Intel Pin, qemu, angr, perf

ACTIVITIES

- **Teaching:** CS296P - Capstone Writing & Communication (Spring '23), CS253P - Advanced Programming and Problem Solving (Fall '19), ICS32 - Programming with Software Libraries (Winter '20)
- **Sub-Reviewer:** IEEE S&P, Usenix Security, NDSS, RAID
- **Capture The Flag:** Member of team **No Internet Access**. Peak rank of 2 in India with multiple top 100 placements in major international CTFs. Responsibilities - reverse engineering, forensics
- **Volunteering:** Taught elementary physics and mathematics to underprivileged high school students as part of Avanti Fellows (NGO) from 2014 - 2017

ACHIEVEMENTS

- **Academia**: Travel Grant - EuroSys (2024), ASPLOS (2024), CCS (2021), Deans Award - UCI (2019), MITACS Globalink Scholarship (2016), Eklavya Scholarship (2015)
- **Industry**: Invitee - Qualcomm Product Security Summit (2023), Letter of Recognition - McAfee (2018), GSoC Mentor - radare2 (2018), Radare Summer of Code (2017), Travel Grant - Clojure Conj (2016)

Revision: December 2024