CHINMAY DESHPANDE

CONTACT INFORMATION

Phone +1 9495612847 **Email** cddeshpa@uci.edu
Github https://github.com/chinmaydd **Website** https://chinmaydd.in

RESEARCH INTERESTS

My primary research interests lie broadly in the area of binary analysis, compilers and systems. I am working on improving the state-of-the-art in binary lifting and recompilation, and more specifically implementing general support for lifting and recompilation of multithreaded binaries. I also like to think about the challenges of IR optimization and refinement in this context.

EDUCATION

University of California Irvine *Fall '19 - Present*
Ph.D. in Computer Science GPA: 3.97/4.0
Advisor: Prof. Michael Franz, Area: Binary Analysis, Compilers and Systems

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

PUBLICATIONS

Chinmay Deshpande, David Gens, and Michael Franz. 2021. StackBERT: Machine Learning Assisted Static Stack Frame Size Recovery on Stripped and Optimized Binaries. In Proceedings of the 14th ACM Workshop on Artificial Intelligence and Security (AISec '21) [paper]

EXPERIENCE

Secure Systems and Software Lab, UC Irvine Research Assistant
Advisor: Prof. Michael Franz *Fall '19 - Present*

- Currently working on BinRec, a framework for binary lifting and recompilation of x86/x64 binaries.
- We are trying to work towards multiple goals in the context of this project - refining generated IR to move away from the "emulator" model, adding compatibility for multithreaded binaries, and incremental lifting being some of them.

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 - where the challenge was to identify interesting taint flows.
- Found and reported multiple bugs in critical QC software. Implemented several 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 (then RMC) Verifier project - which translates Rust programs to equivalent C and uses CBMC for formal verification.

· 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.

Windows Sandboxing (ATD), McAfee Software Development Engineer
Mentor: Sumit Lohani *2017 - 2019*

· Primarily 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

· **Libraries/Software** LLVM, IDA Pro, gdb, OllyDbg, Z3, Intel Pin, qemu, angr

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

ACHIEVEMENTS

· **Academia**: Travel Grant - ACM CCS (2021), Deans Award - UCI (2019), MITACS Globalink Scholarship (2016), Eklavya Scholarship (2015)

· **Industry**: Invitee - QPSS (2023), Letter of Recognition - McAfee (2018), GSoC Mentor - radare2 (2018), Radare Summer of Code (2017), Travel Grant - Clojure Conj (2016)

Revision: September 2023