SUSHANT DINESH

sdinesh2@illinois.edu sushant94 https://sushant94.me/ sushant94

RESEARCH SUMMARY

My research interests are in *program analysis*, *program synthesis*, and securing software against *microarchitectural side-channel attacks*. My work aims to understand how to develop the next-generation of security-centric programming toolflows that enable programmers to write secure (i.e., side-channel resilient) and efficient software on modern (leaky) hardware.

EDUCATION

University of Illinois, Urbana-Champaign *Fall 2019 - Now*
Ph.D. in Computer Science
Advisor: Professor Christopher W. Fletcher

Purdue University *Fall 2016 - Spring 2019*
M.S. in Computer Science
Advisor: Professor Mathias Payer (*Moved to EPFL)*

National Institute of Technology Karnataka, Surathkal *August 2012 - June 2016*
B.Tech. in Computer Engineering

PEER-REVIEWED PUBLICATIONS

- **SynthCT: Towards Portable Constant-Time Code.** *Sushant Dinesh*, Grant Garrett-Grossman, Christopher W. Fletcher. In *28th Annual Network and Distributed System Security Symposium* (**NDSS'22**).
- **RetroWrite: Statically Instrumenting COTS Binaries for Fuzzing and Sanitization.** *Sushant Dinesh*, Nathan Burow, Dongyan Xu, and Mathias Payer. In *IEEE International Symposium on Security and Privacy* (**Oakland'20**).
- **Scalable Validation of Binary Lifters.** Sandeep Dasgupta, *Sushant Dinesh*, Deepan Venkatesh, Vikram S. Adve, and Christopher W. Fletcher. In *Proceedings of the 41st ACM SIGPLAN Conference on Programming Language Design and Implementation* (**PLDI'20**).

RESEARCH EXPERIENCE

FPSG Group, UIUC Research Assistant
Advisor: Prof. Chris Fletcher *2019 - Now*

· Working in the intersection of program analysis, program synthesis, and securing software against microarchitectural side-channel attacks

Microsoft Research - RiSE Research Intern
Mentor: Patrice Godefroid *May 2020 - Aug. 2020*

· Worked on "Tool-assisted interactive Pen-Testing and Verification"
· Push fuzzing more towards verification by exhaustively testing program state-space
· Developed a simple DSL to interactively control symbolic execution during fuzzing
· Using our interactive technique we found several security bugs in development versions of SQL

HexHive Group, Purdue University Research Assistant
Advisor: Prof. Mathias Payer *2016 - 2019*

- Focus on program analysis and its applications to binary rewriting and security
- In depth: worked on static and dynamic program/binary analysis, binary rewriting, reverse engineering, memory safety and sanitizers, and fuzzing

Discover – Binary Component Detection Software Engineering Intern – Research
GrammaTech Inc. Supervisor: Dr. Vineeth Kashyap *Summer/Fall 2018*

- Machine code similarity search that uses a combination of program analysis based features and machine learning. Similarity search is resilient to variation in compilation method, i.e., compiler version and compiler configuration used to build the binary.
- Mainly responsible for: (i) Building all of the machine learning pieces, (ii) Engineering type based features for similarity detection, and (iii) Designing and running experiments for similar component detection.

OPEN SOURCE CONTRIBUTIONS (EXCERPT)

RetroWrite: Statically Instrumenting COTS Binaries for Fuzzing and Sanitization
HexHive Group *2018*

- Sound static binary-rewriting framework for position-independent code
- Implements Binary Address Sanitizer: ASan-like binary-only memory checker
- **Code:** https://github.com/HexHive/retrowrite

Radeco - Binary Analysis Framework Lead Developer / Maintainer
Radare *GSoC 2015, 2016*

- Built the project from ground up. I am responsible for design and implementation of this project
- Implements multiple analysis passes: Symbolization, Dead Code Elimination, Constant Propagation, Basic type inference, Value Set Analysis, and more
- Mentored two students for Google Summer of Code (GSoC) 2018
- **Code:** http://github.com/radareorg/radeco-lib

AWARDS

- Recipient of CS Excellence Award, UIUC for Academic Year 2019 - 2020
- Recipient of Qatar Computing Research Institute and Purdue University Fellowship for 2016 - 2017
- INSPIRE Scholarship for placing in top 1% in AISSCE (2012)

ACTIVITIES

June'19, PI Talk	Presented "Cybertron: Towards Transformation-Based Legacy Software Fitness: Usage-Driven Binary Debloating and Hardening" at Office of Naval Research TPCP meet 2019
Summer'18, Mentor	Google Summer of Code 2018. Project: radeco, Organization: radare
May'18, PI Talk	Presented "Cybertron: Towards Transformation-Based Legacy Software Fitness: Usage-Driven Binary Debloating and Hardening" at Office of Naval Research TPCP meet 2018
April'18	Presented poster on low-overhead binary rewriting at Midwest Security Workshop 2018
September'16	Presented a talk about radeco in r2con, the first radare2 congress *Slides:* https://goo.gl/GT1O8a; *Talk (YouTube):* https://goo.gl/9pfnG7
2013 - 2016	Founded and led undergrad CTF team *No Internet Access*. Multiple top-100 placements in major CTFs

TECHNICAL SKILLS

Languages	Python, C/C++, Rust
Program Analysis	angr, capstone, QEMU, Intel PIN, Datalog, Z3
Reverse Engineering	IDA Pro, radare2, gdb, Olly/ImmunityDBG