SUSHANT DINESH

CONTACT INFORMATION

Phone +1-765-775-8701
Email sdinesh@purdue.edu
Github https://github.com/sushant94
sushant.dinesh94@gmail.com

RESEARCH INTERESTS

My research interests are in the intersection of *program analysis*, *software engineering*, and their applications to *security*. My long term goal is to work in the intersection of these areas to reduce the cognitive load on the programmer and automatically secure applications.

EDUCATION

Purdue University *Fall 2016 - Now*
Ph.D. in Computer Science
Advisor: Professor Mathias Payer

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

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

RESEARCH EXPERIENCE

RetroWrite – Retrofitting Compiler Instrumentation to Blackbox Binaries.

Ph.D. Research *Ongoing*

- Framework for heuristic free static binary rewriting for position independent binaries and libraries.
- Instruments binaries inline and reflows code leading to zero overhead rewriting. Instrumented binaries are as performant as their compiler instrumented counterparts.
- Implemented AddressSanitizer (ASAN) and AFL instrumentation on top of rewriter, enabling low-overhead fuzzing for blackbox binaries.
- To be submitted to Usenix SEC Nov'18.
- Implementation will be open-sourced on acceptance.

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.
- Current results are promising – 90% mean average precision (MAP) in detecting components on test set containing nine popular libraries and 42 variants compiled with different compilers and configurations.

OPEN SOURCE CONTRIBUTIONS

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.
- LLVM-like binary analysis framework with human readable intermediate language (IR)
- 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.
- **Links:** `http://github.com/radareorg/radeco-lib`;

Rune - Symbolic Execution Engine — Lead Developer
Developed as a part of Bachelors' Thesis — *2015 – 2016*

- Developed a library in Rust to interact with SMT solvers such as Z3.
- Developed an interactive symbolic execution engine to symbolically execute small pieces of code.
- Integrated with radare2 to make it a practical tool in a reverse engineer's toolkit.
- **Links:** `http://github.com/sushant94/rune`; `https://github.com/sushant94/libsmt.rs`;

AWARDS

- Recipient of Qatar Computing Research Institute and Purdue University Fellowship for 2016 - 2017.

ACTIVITIES

- Project Mentor. Google Summer of Code 2018. Project: radeco, Organization: radare. **Summer'18**.
- PI Talk. Presented "Cybertron: Towards Transformation-Based Legacy Software Fitness: Usage-Driven Binary Debloating and Hardening" at Office of Naval Research TPCP Kickoff meet. **May'18**.
- Presented poster on low-overhead binary rewriting at Midwest Security Workshop 2018. **April'18**.
- Presented a talk about radeco in r2con, the first radare2 congress. **September'16**.
  Slides: `https://goo.gl/GT1O8a`; *Talk (YouTube):* `https://goo.gl/9pfnG7`