Komail Dharsee

komail.dharsee@gmail.com • https://kdharsee.github.io

Overview

I'm a hardware/software-security researcher with a background in **Computer Science**. I use **formal methods** and **compiler-oriented** techniques to mitigate **low level hardware threats** such as fabrication-time trojans. I'm looking for *research scientist* positions involving compilers, operating systems, architecture, or formal methods.
Skills: C/C++, Rust, LLVM, GDB, SystemVerilog, x86/ARM/RISC-V Assembly, gem5, Python, Coq, Java, Linux

Education

- **University of Rochester**
  PhD, Computer Science — *2016–2023 (Expected)*
- **Rutgers University**
  BS, Computer Science — *2010–2014*

Publications

- **Jinn: Hijacking Safe Programs with Trojans** (UsenixSec '23)
- **Holistic Control-Flow Protection on Real-Time Embedded Systems with Kage** (UsenixSec '22)
- **Fast Execute-only Memory for Embedded Systems** (SecDev '20)
- **Secure Guest Virtual Machine Support in Apparition** (VEE '19)
- **A Software Solution for Hardware Vulnerabilities** (SecDev '17)

Professional Experience

- **University of Rochester**
  Research Assistant — *September 2016–Present*

  Implementing **malicious hardware** that attacks high level software security policies. Modeling **Rust compiler-based** security policies in **SystemVerilog** to identify security critical hardware components. Writing **LLVM Passes** to mitigate vulnerabilities from (1) **memory safety errors** on **ARM microcontrollers**, and (2) **security critical hardware bugs** in **x86 microprocessors**.

- **Pacific Northwest National Laboratory**
  Summer Intern — *March 2020–July 2020*

  Used **Coq** to precisely specify and embed ISA-based security policies in **Kami/Bluespec** microarchitectural designs

- **MIT Lincoln Laboratory**
  Summer Intern — *June 2018–August 2018, June 2019-August 2019*

  Modeled hardware trojans in **Python**. Analyzed hardware trojans detected by sophisticated hardware trojan detection mechanisms (FANCI/UCI/VeriTrust). Identified and designed hardware trojans that enable/evade detection. Designed measures to evaluate detection mechanism reliability based on hardware properties.

- **Acquire Media**
  Software Engineer — *June 2015–August 2016*

  Back-end (**C/C++**) engineer working on the feed handler team. Designed and wrote feed handlers which collect and clean raw feed (commonly received in **XML** or **JSON**) fetched from various web scrapers, ftp sources, and other feed delivery tools. Reviewed colleagues' feed handler implementations prior to release.

- **Rutgers University**
  Undergraduate Assistant Researcher — *September 2012–December 2013*

  Explored the construction of a novel file system that includes new content paradigms hooked to **MongoDB**. Built a prototype **FUSE** user-level file system to allow a dual (shell and MongoDB) file-system interface. Explored the applications of Hadoop cluster programming utilizing the **Map/Reduce** framework towards indexing file systems for search focused application.

Community

- **University of Rochester Strategic Planning Committee** *Grad Rep* — Fall 2021
- **iMentor Workshop (CCS 2020, 2021)** *Mentor* — November 2020, 2021
- **EuroSys 2021** *Shadow PC* — April 2021
- **University of Rochester CS Events Committee** *Chair* — September 2017–August 2021
- **Microsoft** *Student Liaison* — September 2013–June 2014