Harshvardhan Patel

harpatel@cs.stonybrook.edu
harsh1621 | harshvp1621

CAREER SUMMARY: PhD Candidate with over 5 years of industry & research experience in Linux systems programming and security tooling.

- **Professional**: Firmware development and low-level systems programming for embedded Linux systems.
- **Research**: Used static and dynamic program analysis techniques to conduct large-scale vulnerability assessment of Linux open-source software.

EDUCATION

STONY BROOK UNIVERSITY (STATE UNIVERSITY OF NEW YORK) New York, USA
PH.D. IN COMPUTER SCIENCE, GPA: 3.92/4.00 Aug 2022 - May 2027 (expected)
ADVISOR: DR. MICHALIS POLYCHRONAKIS

INDIAN INSTITUTE OF TECHNOLOGY (IIT) BHILAI Chhattisgarh, India
B.TECH IN COMPUTER SCIENCE AND ENGINEERING, GPA: 8.67/10.00 Aug 2016 - May 2020

HONORS & AWARDS

- **RANKED 2ND** , Hofstra-Amazon Capture The Flag (CTF) 2023, Team: BitHammers Nov 2023
- **RANKED 5TH** , (ISC)2 Long Island CTF Competition 2024, Team: BitHammers Mar 2024
- CHAIRMAN'S FELLOWSHIP , Stony Brook University 2022 - 2024
- **RANKED 65TH**, 2018 ACM ICPC REGIONALS - PUNE , India, Team: TLERush Dec 2018

TECHNICAL SKILLS

PROGRAMMING LANGUAGES: Python, Rust, C, Bash, C++
PROGRAM ANALYSIS TOOLS: MIRI, Kani, Ghidra, GDB, LLVM IR
LLM AGENTS DEVELOPMENT: LangGraph
OTHERS: Docker, Capture The Flag (CTF)

PUBLICATIONS

- **Supply Chain Reaction: Enhancing the Precision of Vulnerability Triage using Code Reachability Information** *Harshvardhan Patel, Alexander Snit, Michalis Polychronakis*
  Annual Computer Security Applications Conference (**ACSAC**), 2025 *(Acceptance Rate: 20.6%)*

WORK & RESEARCH EXPERIENCE

TESLA Palo Alto, CA, USA
Security Engineering Intern May 2025 - Aug 2025
Project 1: LLM Agentic workflow for Security Alert Triage

- Developed a **multi-agent LLM workflow** to analyze risks in software dependency upgrades and triage security alerts from static analysis tools across Tesla's code repositories.
- Implemented a **static analysis** pipeline for large codebases (> 700k LoC) to extract security-alert specific context – **vulnerability reachability** information and dependency trees.
- Integrated the tool across 400+ codebases with 2700+ security alerts, significantly reducing alert triage and remediation time. My tool was featured in Tesla's internal Generative AI newsletter.

Project 2: Security and Reliability Tooling for Rust Codebases

- **Formally verified** critical Rust functions using the **Kani** verification tool, identifying and patching *undefined behavior* in critical services.
- Leveraged the dynamic analysis tool **MIRI** to detect *undefined behavior* in third-party dependencies used by internal Rust projects.

HEXLAB | STONY BROOK UNIVERSITY New York, USA
Research Assistant, Advisor: Dr. Michalis Polychronakis May 2023 - present
Project: Function-level Vulnerability Triage for C/C++ binaries .

- Used **static binary analysis** to compute **function-level code reachability** in vulnerable libraries to improve the precision of vulnerability-risk assessment for C/C++ binaries.
- Conducted a **large-scale code-reachability** study on vulnerable C/C++ functions affected by 500+ publicly-disclosed CVEs reported across 24,000+ ELF64 binaries from 6,000+ **Debian packages**.
- Our code-reachability insights showed that for **82%** of these binaries, **at least one CVE reported in their dependencies was unreachable** – a metric overlooked by state-of-the-art scanners that do not inspect software dependencies at function-level.
- Overall for each binary, we identified on average **30%** unreachable vulnerabilities which are falsely reported as reachable by existing scanners that do not perform function-level analysis.

ATONARP MICRO-SYSTEMS Bangalore, India
MEMBER OF TECHNICAL STAFF (FIRMWARE & DEVOPS) Aug 2020 - Jul 2022

- Developed device drivers and patches to customize **embedded Linux kernel** and **U-Boot** bootloader for proprietary hardware.
- Implemented custom Linux kernel module (using Linux RPMSG driver) to enable inter-processor communication for real-time data streaming between ARM Cortex-A (Linux) and Cortex-M (**FreeRTOS**) processors.
- Developed applications to run on the **real-time operating system FreeRTOS**.
- Established secure DevOps practices: built security-hardened **Debian aarch64** images, maintained **Docker** build pipelines, and managed private Debian package repositories.

DE.CI.PHE.RED LAB | IIT BHILAI Chhattisgarh, India
PROJECT SCIENTIST (PART-TIME) Aug 2021 - Mar 2022
Advisor: Dr. Dhiman Saha

- Worked as a part-time Project Scientist for the MEC 5G Test-Bed in collaboration with IIT Delhi.
- Implemented **secure boot** solutions for embedded devices deployed in the test-bed. Implemented **Verified Boot** and **Measured Boot** for Raspberry Pi (RPi) 4 Model B which lacks built-in hardware and software capabilities for secure boot.
- Used an external Trusted Platform Module **(TPM 2.0)** module as the Hardware Root of Trust.
- Patched the open-source bootloader **U-Boot** for RPi to accommodate TPM-based firmware authentication (using TPM2-TSS SDK). Implementation Link: https://github.com/harshvp1621/RPi-TPM-SecBoot

BOSCH-RBEI Bangalore, India
SECURITY INTERN May 2019 - Jul 2019

- Created **minimal & hardened** Linux **Docker** images from scratch for Python applications, achieving **85% size reduction** over standard Docker Hub images.
- **Cythonized** Python applications for performance optimization and developed automated build pipelines using Bash and Bazel.
- Built security-focused **distroless** container images by packaging only essential runtime dependencies, significantly reducing the attack surface.

MAX SECURE SOFTWARE Pune, India
SOFTWARE DEVELOPMENT INTERN (ANTIVIRUS TEAM) May 2018 - Jul 2018

- Developed and deployed a **malware classifier** for Windows executables using random forests algorithm, achieving high accuracy through 30+ statically extracted features. Integrated the classifier as a Windows dynamic link library (DLL) to the company's antivirus product.
- Created a proof-of-concept for **Android malware detection** using features extracted from APK manifests and Dex files, laying groundwork for company's Android threat detection capabilities.