Prakhar Sah PhD Student

sprakhar@vt.edu
https://prakhar-sah.github.io

Research Interests

With an experience of 3+ years in the areas of Computer Architecture, Embedded Systems and Security, my research projects range from firmware level security to hardware/software co-design. In particular, I am interested in evaluating and strengthening the security of systems in resource-constrained and untrusted environments.

Education

PhD, Computer Science 2023 - 2026 *(expected)*
Virginia Tech **Advisor:** Dr. Matthew Hicks

MS, Electrical and Computer Engineering 2021 - 2023
Virginia Tech GPA: 3.8/4.0

BS, Electronics and Telecommunication Engineering 2017 - 2021
Dwarkadas J. Sangvhi College of Engineering GPA: 7.8/10.0

Professional Experience

Virginia Tech | Graduate Research Assistant 2021-Present

- Design and evaluate trusted execution and context management techniques in resource-constrained environments.
- Investigate trade offs between security and performance of checkpointing techniques in intermittently powered batteryless devices.
- Explore the vulnerability space of ultra-low size, weight and power microcontroller trusted execution environments.

Arm | Productivity Engineering Intern Summer 2024

- Improved the Medini threat modelling process of HSDL (Hardware Secure Development Lifecycle) used in 50+ Arm products.
- Integrated support for Architecture and Technology Group security risk assessment and system microarchitecture threat models.
- Contributed to an in-house microarchitecture vulnerability pen testing tool based on functional verification techniques.

NTPC | Software Engineering Intern Winter 2020

- Automated the file accessing system and integrated it with the a calendar widget using Javascript.
- Built the database model and front-end design for the company website using ASP.NET MVC and SQL server.

Technical Skills

- Hardware/software co-design • Firmware Security • Intermittent Computation
- Threat Modeling & Risk Assessment • TEE: Texas Instruments MSP IP Encapsulation
- AMD Vivado Design Suite, Code Composer Studio, mspdebug, GCC, ANSYS Medini
- C, Assembly (RISC-V, ARM), Verilog, Python, Javascript

Publications

RIPencapsulation: Defeating IP Encapsulation on TI MSP Devices. Prakhar Sah and Matthew Hicks. USENIX WOOT Conference on Offensive Technologies (**WOOT**). August 2024.

Hitchhiker's Guide to Secure Checkpointing on Energy-Harvesting Systems. Prakhar Sah and Matthew Hicks. International Workshop on Energy Harvesting & Energy-Neutral Sensing Systems (**ENSsys**). November 2023.

Research Projects

Interrupt-based Side-channel Attacks against Commercial TEEs: Texas Instruments' MSP IP Encapsulation aims to provide confidentiality of data stored inside the IPE memory zone; this includes proprietary code and keys. I devised exploits that break this guarantee by leveraging two fundamental drawbacks in IPE design: residual state on context switches and lack of call site verification. **Outcome:** One conference paper (USENIX WOOT '24)

A Survey of Secure Checkpointing Techniques in Energy-harvesting Devices: A qualitative comparison of adopted threat models, security guarantees and resource utilization of popular secure checkpointing techniques used in energy-harvesting devices. This study reveals that most of the secure checkpointing techniques do not consider an adversary with physical access which is a common occurrence in real-world IoT deployments. It postulates a more realistic adversarial model for reliable defensive strategy that is practical in terms of deployment, flexibility, and energy consciousness. **Outcome:** One workshop paper (ENSsys '23)

Other Projects

Energy Harvesting and Intermittent Computing: Designed my own checkpoint management system trading off resource availability and freshness across non-deterministic power cycles and evaluated forward progress of embedded crypto benchmarks on recorded energy harvesting power traces.

Implementation and Evaluation of a Polling Server on ATmega2560: Designed a polling server, evaluated response times for aperiodic & sporadic tasks, compared EDF, RMS, DMS algorithms.

Implementation and Mitigation of Spectre Attacks on RISC-V Microarchitecture: Replicated Spectre PHT & RSB on RISC-V BOOM core and explored mitigation strategies.

Object Detecting Autonomous Water Vehicle: Designed robot navigation with SLAM, established remote encoder access, interfaced sensors and actuators with the MCU.

Presentation & Talks

RIPencapsulation: Defeating IP Encapsulation on TI MSP Devices. (WOOT) 2024

Hitchhiker's Guide to Secure Checkpointing on Energy-Harvesting Systems. (ENSsys) 2023