ASMITA

aasmita@ucdavis.edu • linkedin.com/in/asmita-a • github.com/asmitaj08 • asmitaj08.github.io

EDUCATION

PhD Candidate in Electrical & Computer Engineering
University of California, Davis Sept 2021 - Sept 2025
• Graduate student researcher : Improving embedded firmware security assessment techniques using Fuzzing
• Teaching Assistant (TA) : Embedded System Courses (EEC007 x5, EEC172 x3) - Conducting microcontroller lab sessions
• Research Overview : Utilizing fuzzing techniques to uncover vulnerabilities in bare-metal firmware, developing automation framework, contributing towards improving firmware fuzzing techniques and exploring how LLM can be leveraged in this domain : Link

MS in Electrical & Computer Engineering
University of California, Davis 2021-23
Relevant courses : Computer security, Hardware security, Embedded computing, Computer architecture, Machine Learning, Digital system testing, Internet of Things (IoT) (GPA: 3.95)

Bachelor of Engineering in Electronics
International Institute of Information Technology, Pune, India 2014-18

SKILLS

Python, C, Firmware static & dynamic analysis, Fuzzing, Emulation, Firmware reverse engineering, Embedded systems, Firmware security | IoT security | Embedded security; Firmware security tools - Qemu, Unicorn, Renode, AFL/AFL++, LibAFL, Ghidra, Binwalk, Angr and others; Firmware extraction using JTAG, SWD, flash dump; Shell access via UART; Vulnerability research and penetration testing; Secure code review; Product security assessment

WORK EXPERIENCE

Product Security Intern — AMD, USA Summer 2024
• Developed fuzzer for AMD GPU Kernel Fusion Driver (KFD) IOCTL. • Performed random hardware fuzzing via debug interface to change the state of the device under test. • Performed C/C++ secure code review as part of product security assessment

Firmware Security Intern — NetRise, USA Summer 2023
• Conducted research on IoT firmware fuzzing techniques, including AFL++, LibFuzzer, LibAFL, and OSS-Fuzz, while also investigating the usage of LLMs in fuzzing. • Assisted NetRise in the development of an initial test prototype (in Python) to integrate firmware fuzzing into their existing framework. • Conducted comprehensive testing on 263 Busybox packages, identifying potential vulnerabilities for mitigation.

Firmware Security Intern — NetRise, USA Summer 2022
• Research and implementation for Control Flow Graph-based static analysis and prototyped binary function similarity using Python. • Assisted NetRise in creating a Proof of Concept (PoC) for adding binary similarity identification features to their framework, enhancing the identification of third-party software components more robustly.

IoT Security Consultant — Payatu, India Oct'19 to Sept'21
• Conducted security assessments and penetration testing on diverse IoT products, including smart cameras, medical devices, wireless modems, and ECUs. • Worked with various static & dynamic analysis tools including Ghidra, Binwalk, Qemu, Unicorn, AFL++, Firmadyne, and others • Served as a security architect for an automotive client, integrating security into product design. • Trainer for IoT Hacking Training : Trained approx 50-100 participants at global conferences. • Assisted Payatu in efficiently delivering security assessment outcomes to their clients and expand their training programs across different organizations.

PUBLICATIONS

1. **Asmita**,Y. Ollinyk, M. Scott, R. Tsang, C. Fang, H. Homayoun. "Fuzzing BusyBox: Leveraging LLM and Crash Reuse for Embedded Bug Unearthing." Usenix 2024 - Link.
2. R. Tsang, **Asmita**,D. Joseph, S. Salehi, P. Mohaptra, H. Homayoun. "FFXE: Dynamic Control Flow Graph Recovery for Embedded Firmware Binaries." Usenix 2023 - Link.
3. R. Tsang, D. Joseph, **Asmita**, S. Salehi, P. Mohaptra, H. Homayoun. "FANDEMIC: Firmware Attack Construction and Deployment on Power Management IC and Impacts on IoT Applications." NDSS 2022. - Link

PROJECTS & PARTICIPATIONS

Bare-metal Firmware Fuzzing Framework (*In progress*): Developing a framework to leverage LibAFL fuzzer and Renode emulator for fuzzing embedded targets. In parallel, exploring how to leverage LLM for fuzzing embedded targets.
IOSC2: IoT Firmware Security : Performed analysis on a dataset of 107 real-world firmware binaries for identifying third-party software components and corresponding CVEs. — Contributed to firmware dataset collection, automation script development, and analysis. — GitHub Link
Binary Similarity Project : Implemented machine learning algorithms to determine the similarity between binary functions. — Contributions included dataset generation, feature extraction from binary control flow graphs (CFGs), feature vectorization, and applying MLP and CNN algorithms. — GitHub Link
Google HardPwn Contest : Achieved root access on the Google Pixel watch during the challenging HardPwn contest orgainized by Google at Hardwear.io. — Link
CTFs : Top 50 in Cyber Defense Challenge organised by Target and WiCyS — Link
Google Cybersecurity Specialization : Completed this course by Google on Coursera — Link