# ASMITA

(530)-231-2285 ◇ 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 - Present
Graduate student researcher : Improving embedded firmware security assessment techniques.
Teaching Assistant (TA) : Embedded System Courses (EEC007 x3, EEC172 x2) - Engaging lab sessions
Research Overview : Utilizing fuzzing techniques to uncover vulnerabilities in bare-metal firmware, addressing firmware fuzzing challenges, and contributing towards improving firmware security assessments techniques. Details

**MS in Electrical & Computer Engineering**
University of California, Davis — 2021-23
Relevant courses : Computer security, Hardware security, Embedded computing, Computer architecure, 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, Qiling, AFL/AFL++, LibAFL, LibFuzzer, OSS-Fuzz, Ghidra, Radare, Binwalk, Avatar, Firmadyne

## WORK EXPERIENCE

**Firmware Sceurity 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 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
- Embedded hardware and firmware security assessments including IoT protocol, and basic side-channel & fault injection attacks. — Conducted security assessments on diverse IoT products, including smart cameras, medical devices, access control systems, wireless modems, and ECUs. — 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 Nullcon, CPX360 Checkpoint.
- Assisted Payatu in efficiently delivering security assessment outcomes to their clients and expand their training programs across different organizations.

## PUBLICATIONS

1. R. Tsang, **Asmita**,D. Joseph, S. Salehi, P. Mohaptra, H. Homayoun. "FFXE: Dynamic Control Flow Graph Recovery for Embedded Firmware Binaries." Usenix 2023 - Link.
2. 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

**IOSC2: IoT Firmware Security** : Performed in-depth static analysis on a dataset of 107 real-world firmware binaries. — Contributed to firmware dataset collection, automation script development, and comprehensive analysis. — GitHub Link

**OS-Based Firmware Unveil** : Developed an all-in-one automated platform for extracting static information from Linux-based IoT firmware. — Contributed to the development of this platform using tools like Binwalk, Firmwalker, and Cve-bin-tool. — 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

**Identify Memory Corruption Bugs using Fuzzing** : Delved into existing firmware analysis tools and experimented with fuzzing and symbolic execution techniques (AFL++ and SymCC) — Doc Link

## ACHIEVEMENTS

- Achieved root access on Google Pixel watch : HardPwn Contest by Google. — May 2023
- IEEE Best Teaching Assistant (TA) Award, UC Davis. — Sept 2022
- Best Outgoing Student & Academic Topper Award. — June 2018
- Best Paper Award at CEET, Kuala Lumpur, Malaysia. — April 2018
- AIT-Tiger Leong International Innovation and Leadership Camp — July 2017
- Invited talks and workshops : asmitaj08.github.io/trainings-and-talks/