SAASTHA VASAN

2114 Harold Frank Hall, Santa Barbara, CA 93106-5110
saastha@ucsb.edu — https://github.com/saasthavasan

RESEARCH OVERVIEW

My research focuses on the intersection of machine learning and computer security, frequently integrating concepts from program analysis. In general, my work aims to develop innovative frameworks that surpass existing methods in the field of malware analysis and vulnerability assessment.

EDUCATION

University of California, Santa Barbara Sept 2021 - Present
Doctor of Philosophy(Ph.D), Computer Science, CGPA: 3.9/4.0

Amrita Vishwa Vidyapeetham, Kerala, India Jul 2016 - Jul 2020
Bachelor of Technology, Computer Science

WORK EXPERIENCE

Graduate Researcher Sept 2021 - Present
Security Lab, UC Santa Barbara *Santa Barbara, California*

- Performing independent and collaborative research in malware analysis, threat intelligence, and LLMs for vulnerability assessment.
- Authoring academic papers and journals for top system security conferences.
- Participating in Capture The Flag (CTF) competitions as a member of team Shellphish.

Infosec Engineer December 2020 - July 2021
Aspirify Inc *New Delhi, India*

- Developed in-house tools and techniques for red teaming.
- Conducted malware analysis and reverse engineering to identify impact and removal strategies.

Research Intern March 2020 - September 2020
Security Lab, UC Santa Barbara *Santa Barbara, California*

- Created an automated post-detection framework to identify capabilities in Windows malware.
- Reverse-engineered malware executables and mapped their attack implementations to the MITRE ATT&CK Framework.

Student Researcher Oct 2016 - March 2020
Security Lab, Amrita Vishwa Vidyapeetham *Kerala, India*

- Analyzed malware, documented findings, and implemented proof-of-concept attack techniques.
- Actively participated in Capture The Flag (CTF) challenges as a member of team bi0s.

PROJECTS & PUBLICATIONS

- **Large Malware Model**: A multi-modal LLM to characterize malware using static features.
- **DeepCapa**: An automated post-detection framework to identify capabilities in Windows malware.
- **WatermarkAttacker**: A family of regeneration attacks to remove invisible watermarks in images.
- **CbDroid**: A callback level coverage-guided fuzzing framework to perform stress testing on Android applications.
- **PHPIL**: A fuzzing framework for the PHP interpreter to discover memory corruption bugs.

ACHIEVEMENTS

- **Academic Excellence Fellowship (2021)** University of California, Santa Barbara.
- **Graduated magna cum laude (2020)**, Amrita Vishwa Vidyapeetham.
- **Student Excellence Award Winner (2018, 2019)**, Amrita Vishwa Vidyapeetham.

TECHNICAL SKILLS AND LANGUAGES

Programming Languages	Python, C, C++, x86 Assembly
Software and Frameworks	Pytorch, IDA, Ghidra, x64dbg, GDB
Languages	Hindi(native), English(fluent), Tamil(fluent)