SAASTHA VASAN

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

RESEARCH OVERVIEW

My research focuses on the intersection of machine learning and computer security, frequently integrating concepts from program analysis. My work aims to create novel frameworks that surpass current methodologies in the domains 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*

- Collaborated with the in-house red team to develop and maintain a red teaming framework.
- Developed new modules to increase the attack surface, enhancing the effectiveness of red teaming efforts.
- Ensured the compatibility of existing modules and maintained the effectiveness of the framework in an evolving threat landscape.

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

- Designed and developed a novel malware post-detection framework that identifies potentially malicious capabilities in Windows malware, outperforming existing solutions by 20% in precision and 80% in recall.
- 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*

- Conducted malware analysis, documented results, and developed proof-of-concept attack methods.
- Fostered collaborative learning by teaching reverse engineering and malware analysis, promoting ongoing education.
- Participated actively in Capture The Flag (CTF) competitions as part 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 (2018, 2019)**, Amrita Vishwa Vidyapeetham.

TECHNICAL SKILLS AND LANGUAGES

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