2114 Harold Frank Hall
Santa Barbara, CA 93106-5110
☎ *+1 (805) 837 5785*
✉ *saastha@ucsb.edu*
🌐 *saasthavasan.github.io*
saasthavasan
in *saasthavasan*

Saastha Vasan

Ph.D. Candidate in Computer Science

Research Overview

My research focuses on the application of artificial intelligence (AI) for cybersecurity. Specifically, my work aims to create novel frameworks using AI that surpass existing methodologies in the domains of malware analysis and vulnerability assessment.

Education

Sept 2021 – Present
Doctor of Philosophy (Ph.D.) in Computer Science, *University of California, Santa Barbara*
Advisors: Prof. Giovanni Vigna and Prof. Christopher Kruegel

July 2016 – July 2020
Bachelor of Technology in Computer Science, *Amrita Vishwa Vidyapeetham*, Kerala, India

Research Experience

Sept 2021 – Present
Graduate Researcher, 🌐 *Seclab, UC Santa Barbara*, Santa Barbara, CA

- Conducting research on the application of AI in cybersecurity, with a focus on advancing techniques for **malware analysis**, **threat detection**, and **vulnerability assessment**.
- Submitting papers to top peer-reviewed security conferences.

Mar 2020 – Sept 2020
Research Intern, 🌐 *Seclab, UC Santa Barbara*, Santa Barbara, CA

- Researched on AI methods for **malware post-detection** analysis.
- Designed an automated framework for identifying malicious capabilities in Windows malware.

Oct 2016 – Mar 2020
Student Researcher, *Security Lab, Amrita Vishwa Vidyapeetham*, Kerala, India

- Carried out **malware analysis** and documented the findings.
- Actively participated in Capture The Flag (CTF) competitions as a member of the team **bi0s**, leading **reverse engineering** efforts.

Industry Experience

Dec 2020 – July 2021
Infosec Engineer, *Aspirify Pvt. Ltd.*, New Delhi, India

- Developed new modules for RCE, lateral movement, and N-day vulnerabilities for the existing red teaming framework using C, C++, C#, and Python.
- Expanded the framework's capabilities, leading to an increased customer base.

Publications

Under Review
MalwarePT: A Robust Binary-Level Foundation Model for Malware Analysis, *Submitted to 46th IEEE Symposium on Security and Privacy (IEEE S&P 2025)*

- MalwarePT is a BERT-based foundation model designed to learn the representations of raw bytes within the code segment of executable files. It surpasses existing malware analysis models in terms of **generalizability** and **adversarial robustness**, while preserving similar performance in malware detection and functionality classification tasks.
- **Authors: Saastha Vasan**, Yuzhou Nie, Kaie Chen, Hojjat Aghakhani, Yigitcan Kaya, Wenbo Guo, Christopher Kruegel, Giovanni Vigna

2024
DeepCapa: Identifying Malicious Capabilities in Windows Malware, *40th Annual Computer Security Applications Conference (ACSAC 2024)*

- DeepCapa is a malware post-detection framework that detects malicious capabilities in Windows malware. It maps API call sequences to malicious capabilities (**MITRE ATT&CK** techniques) using static analysis and neural networks.
- **Authors: Saastha Vasan**, Hojjat Aghakhani, Stefano Ortolani, Roman Vasilenko, Ilya Grishchenko, Christopher Kruegel, Giovanni Vigna

2024 **Invisible Image Watermarks Are Provably Removable Using Generative AI**, *38th Annual Conference on Neural Information Processing Systems (NeurIPS 2024)*

- ○ Propose a family of **regeneration attacks** using generative AI to remove invisible watermarks from images. The attack adds random noise and reconstructs the image via generative models, demonstrating that such watermarks are provably removable compared to traditional methods.
- ○ **Authors:** Xuandong Zhao, Kexun Zhang, Zihao Su, **Saastha Vasan**, Ilya Grishchenko, Christopher Kruegel, Giovanni Vigna, Yu-Xiang Wang, Lei Li

2023 **COLUMBUS: Android App Testing Through Systematic Callback Exploration**, *45th International Conference on Software Engineering (ICSE 2023)*

- ○ COLUMBUS is a callback-driven fuzzer designed to improve the code coverage by systematically exploring callbacks in Android applications. It employs symbolic execution and dynamic heap introspection to generate arguments for callbacks, resulting in more effective stress testing.
- ○ **Authors:** Priyanka Bose, Dipanjan Das, **Saastha Vasan**, Sebastiano Mariani, Ilya Grishchenko, Andrea Continella, Antonio Bianchi, Christopher Kruegel, Giovanni Vigna

2020 **PHPIL: Fuzzing the PHP Interpreter with Custom Bytecode**, *11th International Conference on Computing and Networking Technology (ICCNT 2020)*

- ○ PHPIL is a fuzz-testing framework designed to detect vulnerabilities in PHP engines. PHPIL proposes an intermediate language to generate syntactically valid and semantically meaningful PHP programs, which improves the discovery of security vulnerabilities.
- ○ **Authors:** V. S. Rao, Tarunkant Gupta, **Saastha Vasan**, Deepthi L.R

Current Research

C2F2: An LLM-assisted framework for generating deployable network traffic signatures to detect various open-source and closed-source **C&C** frameworks at endpoints.

AI for Cyber Threat Intelligence: The study aims to systematize the various stages of the **cyber threat intelligence** (CTI) lifecycle, evaluating the current application of AI techniques, and propose new research directions to enhance **CTI generation**, **CTI sharing**, and **CTI application**.

Universal Debugger: An LLM-powered agent designed to interface with a debugger and perform **root-cause** analysis of crashes identified during fuzz-testing.

Patcher-Q: A multi-agent LLM framework for **root-cause** analysis and **patch generation** of security vulnerabilities.

Stimulus: A framework designed to augment **CodeQL** by identifying code patterns where it fails and leveraging an LLM to rewrite the code for more precise analysis.

Additional Experience

🌐 **AI Cyber Challenge (AIxCC) – [2023 - Present]**: As part of team **Shellphish**, I contributed to developing systems for root-cause analysis and vulnerability patching. Our team secured a top-7 finish in the semi-finals, winning **$2 million** and advancing to the finals.

🌐 **NSF ACTION Institute Student Executive Council – [2023 - Present]**: Serving as a student representative responsible for managing **internship recruitment**, coordinating guest **speaker sessions**, fostering **research collaborations** between universities, and leading **outreach efforts** to teach AI and security to high school students.

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

Programming	Python, C, C++, x86 Assembly
Frameworks	PyTorch, IDA Pro, x64dbg, GDB, YARA
Languages	Hindi (Native), English (Fluent), Tamil (Fluent)