

Karthik Ramakrishnan

SECURITY RESEARCHER

✉ rkarthik@gatech.edu | 🏠 karthikr.in | 📧 L3thal14 | 📺 karthikr1406 | 🎓 Karthik Ramakrishnan

About Me

My research examines web security and privacy issues through empirical measurements. My focus on data-driven approaches aim to evaluate how current online systems impact users. Through these methods, I aim to derive insights that can inform the design of more effective Web security and privacy solutions.

I am currently exploring the security and privacy implications of LLM agents, including web agents and computer-use agents, and also focusing on detection mechanisms for automated agent interactions

Education

Georgia Institute of Technology

Atlanta, U.S.A

Doctor of Philosophy in Computer Science

2024 - 2028

Advisor: **Prof. Frank Li**

Area of Research: Web security, privacy and Internet measurement, LLM Agents

Georgia Institute of Technology

Atlanta, U.S.A

Master of Science in Cybersecurity

2022 - 2024

Advisor: **Prof. Frank Li**

Area of Research: Web security, privacy and Internet measurement

Manipal Institute of Technology

Manipal, India

B.Tech Electronics and Communication Engineering with a minor in Computing

2018 - 2022

Thesis: Browser Fingerprinting Detection and Mitigation Framework

Work / Research Experience

Georgia Institute of Technology

Atlanta, U.S.A

Graduate Research assistant, Advisor: **Prof. Frank Li**

August 2022 - Present

- **AI Agentic Abuse** - Currently working on measuring how susceptible frontier AI web agents are to being manipulated into carrying out harmful real-world tasks, and on defenses against such abuse.
- **Website Passkey Adoption** - Worked on a large-scale study measuring how websites adopt and communicate passkeys, a passwordless login method, using a search-augmented LLM to analyze their documentation.
- **Web Privacy crawler configurations** - Worked on evaluating crawler configurations for web privacy measurement studies.

CISPA Helmholtz Center for Information Security

Saarbrücken, Germany

Research Intern, Advisor: **Dr.-Ing. Ben Stock**

June 2023 - August 2023

- Extended the Web Platform Tests (WPT) suite to include support for generated invalid test cases for headers.
- Worked on manually investigating inconsistencies in HTTP Header parsing implementations across different browsers across both desktop and mobile platforms.
- Work has been accepted to ACM CCS 2025.

IMDEA Software Institute

Madrid, Spain

Research Intern (Bachelor Thesis), Advisors: **Dr. Juan Caballero & Dr. Srdjan Matic**

February 2022 - July 2022

- Worked on design, development, and evaluation of a framework for analyzing browser fingerprinting techniques and their countermeasures using Chrome Devtools Protocol (CDP) as part of my Bachelor thesis.
- Developed a CDP Proxy to intercept messages received and sent by the Devtools client in real-time. This also involved evade detection of CDP usage employed by scripts on websites.
- Developed an initial prototype to parse the protocol logs to link responsible scripts with web API calls by constructing a graph representation of the same.

- Worked on developing a custom deployable production HoneyPot with Visualisation Dashboard for non-technical users.
- I was also involved in creating an incident response training curriculum for executives and the tech team of companies.
- Presented the research output at the CyberVSR Symposium 2021.

Research Publications

Anonymous Authors.

Understanding Website Passkey Policies and User Communication

Under submission ACM Conference on Computer and Communications Security (CCS), 2026.

Karthik Ramakrishnan, Qing Xie, Uma Anand, Frank Li

Crawling in the Deep: Evaluating Web Crawling Configurations for Web Privacy Measurements

ACM Internet Measurement Conference (IMC), 2026.

Jannis Rautenstrauch, Trung Tin Nguyen, **Karthik Ramakrishnan**, and Ben Stock

Head(er)s Up! Detecting Security Header Inconsistencies in Browsers

ACM Conference on Computer and Communications Security (CCS), 2025.

Qing Xie, **Karthik Ramakrishnan**, and Frank Li

Evaluating Privacy Policies under Modern Privacy Laws At Scale: An LLM-Based Automated Approach

USENIX Security Symposium 2025

Dhruv Kuchhal, **Karthik Ramakrishnan**, and Frank Li

Whatcha Lookin' At: Investigating Third-Party Web Content in Popular Android Apps.

ACM Internet Measurement Conference (IMC), 2024.

Achievements/Honors

- | | |
|------|--|
| 2023 | NDSS Symposium 2023 Student Support Award , Awarded to 17 students out of 80+ applicants |
| 2021 | Cybersecurity Visiting Student Research (CyberVSR) Scholar , Rochester Institute of Technology |
| 2020 | National Finalist(Top 150) , InCTF 2020 Capture The Flag(CTF) Competition |
| 2018 | Linux Foundation Training Scholar , Awarded by Linux Foundation for contributions towards open-source |
| 2016 | Finalist(Top 500 Startups and Groups) , Hello Tomorrow Entrepreneurship Challenge |
| 2016 | Winner , InoVIT Science Fair (Project Showcase Category) |
| 2016 | National Finalist (Top 100) , Intel IRIS Science Fair |
| 2015 | Regional Finalist (Top 90 across the world) , Google Science Fair |

Skills

Languages: Python, JavaScript(ES6), HTML, CSS/Sass, Bash, $\text{\LaTeX}$

Software/Libraries: Selenium, Playwright, Flask, Django, Docker, MongoDB

AI tools: Claude Code, Cursor, Codex CLI, Web Agents