

RITIK ROONGTA

✉ ritik.r@nyu.edu | 🌐 Racro | 🌐 racro.github.io | 🌐 Ritik | 📍 San Jose, CA, USA

Research Statement

I aim to build **open source** frameworks that create real world impact while advancing academic research. I focus on transforming digital advertising through **automated content** moderation and **detecting malicious actors** in the ad supply chain. My past work includes **empirical** studies on privacy-enhancing technologies, propaganda, and harmful ads; using AI to **detect** contextual nuances and **mitigate** these issues at scale.

Going forward, I aim to enhance user experience online by uncovering differential treatment, **fighting fraud**, and conducting **large scale measurements** to improve widely used tools.

Education

New York University (NYU)

Ph.D. in Computer Science, Advisor: Prof. R. Greenstadt & Prof. B.D. Gavitt

Thesis: Adblocking's Privacy Tradeoffs and the Future of Sustainable Advertising

Sep '21 – Jun '26

New York City, USA

Indian Institute of Technology Bombay (IITB)

B.Tech in Computer Science, GPA: 8.15/10.0

Thesis: Large-scale assessment of vulnerabilities in open-source network server binaries

Sep '17 – May '21

Mumbai, India

Publications

AdLens: Efficient Detection of Deceptive Software Ads

CCS '26

Ritik Roongta, M.A. Darwish, M.A. Aghdam, R. Greenstadt and G. Acar

Paper | Code | Poster

- Designed an open-source, multilingual two-stage LLM pipeline that audits ad transparency libraries at scale, cutting inference cost 17x versus exhaustive classification while achieving 0.92 F1
- Used it to expose thousands of deceptive software ads and the malvertising campaigns hidden behind them, leading to takedowns after disclosure to Google

Automated detection and evaluation of problematic ‘allowed’ advertisements

PETS '25

Ritik Roongta, Julia Jose, Hussam Habib and Rachel Greenstadt

Paper | Code | Poster

- Developed an LLM-assisted Ad content moderation framework to enable adblockers to detect problematic ads and block them, thus protecting users from excessive tracking and intrusive advertising

When Agents Persuade: Rhetoric Generation and Mitigation in LLMs

AIWILD, ICLR '26

Julia Jose, Ritik Roongta and Rachel Greenstadt

Poster

- Uncovered the potential of LLMs in generating propaganda and designed NLP-based frameworks to efficiently detect and mitigate them, shielding users from false and fake content

A User-Focused Evaluation of Privacy-Preserving Browser Extensions

AsiaCCS '24

Ritik Roongta and Rachel Greenstadt

Paper | Code

- Built a usability and privacy framework to evaluate privacy-preserving extensions on performance, permission abuse, web compatibility, etc., aiding the users in making informed choices

Analysis of web breakages caused by adblockers

SecWeb, IEEE S&P '24

Ritik Roongta, Mitchell Zhou, Ben Stock and Rachel Greenstadt

Paper | Code

- Conducted web measurement experiments to quantify web breakages caused by adblockers across five different categories, thus improving the state of web for adblocker users

Drifuzz: Harvesting Bugs in Device Drivers from Golden Seeds

USENIX '22

Zekun Shen, Ritik Roongta, and Brendan Dolan-Gavitt

Paper | Code

- Implemented a framework for concolic fuzzing PCI device drivers, discovering and patching **12 bugs** and obtained **2 CVEs** in the Linux driver code, leading to a bug-free operating system

Work Experience

Palo Alto Networks

Aug '26 – Present

Sr. Staff Web Security Researcher | Guide: Oleksii Alex Starov

Suanta Clara, US

- Part of the Advanced URL filtering team handling malicious web URLs including JS, HTML, etc.

Uber Technologies

Sep – Nov '25

PhD Software Intern | Guide: Xandra Xhu & Bo Ling

Sunnyvale, US

- Implemented a LLM-based generative recommender model for UberEats homefeed for tar-aware predictions
- Developed TPU and GPU comptiable frameworks for geenrative recommenders models for efficient hardware benchmarking achieving 5.3x higher throughput on TPUs

CISPA Helmholtz Center for Information Security

Jun – Aug '24

Research Intern | Guide: Ben Stock

Saarbruecken, Germany

- Developed a novel mechanism to identify the differential treatment of adblocker users by websites, uncover potential for fingerprinting users and degrading their user experience
- Instrumented the Google Chrome's V8 engine to collect JS execution logs to understand its inner workings

University of California, Santa Barbara

Apr – Nov '20

Research Intern | Guide: Giovanni Vigna and Christopher Kruegel

Santa Barbara, USA

- Developed **KANF**, a kernel-assisted network fuzzer, using Linux kernel driver modules and networking tools to test **over 10,000** open-source network programs and conduct bug detection at scale
- Interleaved the Linux Kernel with (**AFL**) using kernel driver modules and network programs

A.P.T Portfolio

Apr – Jun '20

Software Engineer Intern | Guide: Pratyush Rathore

Delhi, India

- Reported and **patched** crucial **bugs** in the source code implemented for processing a daily **traffic** in excess of **4 crores** orders at NSE and developed and optimized **dynamic latency** based exchange simulation model

Lucideus

May – Jul '19

Cyber Security Research Intern | Guide: Rahul Tyagi

Delhi, India

- **Hardened** CentOS linux using 239 remediations as provided by **CIS** (Center for Internet Security) and prepared a detailed documentation covering attacks and mitigation techniques on **OWASP** Top 10 Attacks

Reviewer Duties

Program Committee: NDSS '25, PETS '24, MADWEB '25

Artifact Committee: CCS '24/25, USENIX '23/24, PETS '25

Technical Skills

ML Paradigms:	Natural Language Processing, Prompt Engineering, Sentiment Analysis, Thematic Analysis, Supervised/Undepervised Learning, RAG
ML Frameworks:	PyTorch, LLMs, VLMs, NumPy, Pandas, Jupyter
Internet Measurement:	Puppeteer, Selenium, Playwright, Web Extensions
Languages:	C/C++, Python, Bash, Java, Assembly, JavaScript
Security Tools:	Kali Linux, Metasploit Framework, Xerosploit, Reversing Tools
Software tools:	Linux, Git, MATLAB, MySQL, AutoCAD, L ^A T _E X, AWS, HPC, Slurm

Position of Responsibility

Teaching Assistant

Jan '22 - Apr '22

New York University | *Application Security*

New York, USA

- Mentored a class of over 100 students in a remote setup for the Application Security course and facilitated practical class demonstrations to instill a better understanding of niche concepts

Thesis Mentor

Sept '23 - May '24

Real-time measurement of web breakages | Mitchell Zhou

New York University, USA

- Mentored an undergraduate student for his bachelor's thesis on understanding web breakages and measuring them on large-scale, leading to a publication at SecWeb, IEEE S&P

Awards / Leadership

- Presented research posters Columbia Privacy day and Google Ad Privacy day [2025]
- Received a **scholarship** to attend summer school in EPFL, Switzerland and CISPA, Germany [2024]
- Received **SoE** fellowship from NYU in my freshmen year to facilitate my research goals [2021]
- Secured All India Rank **48** in **JEE-Advanced** out of 220,000 shortlisted candidates [2017]
- Awarded **KVPY** Fellowship and **NTSE** Scholarship by the Government of India [2016]