Ritik Roongta

Brooklyn, NY, USA | Racro | Ritik | racro.github.io | ritik.r@nyu.edu

Education

New York University **Sep ’21 – May ’26**
Ph.D. in Computer Science, Advisor: Prof. Rachel Greenstadt & Prof. Brendan Dolan Gavitt *New York City, USA*

New York University **Sep ’21 – May ’23**
MS in Computer Science, GPA: 4.0/4.0 *New York City, USA*

IIT Bombay **Sep ’17 – May ’21**
B.Tech in Computer Science, GPA: 8.15/10.0 *Mumbai, India*

Publications

Effective and Inclusive Ad Moderation — Jan ’25

Ritik Roongta, Julia Jose, Hussam Habib and Rachel Greenstadt *CCS*

- Developed a fine-grained taxonomy using **NLP** and **manual analysis** aimed at accommodating the interests of all advertising stakeholders and enabling scalable moderation of problematic content via LLMs
- Established the potential of LLMs for large scale ad content moderation by achieving an agreement score of **0.75** with the ground truth
- Uncovered the widespread presence of problematic ad content on the web (30%) using LLMs over **10k** ads
- Enhanced existing web crawlers to collect ads authenticated profiles and minimize confounding variables

Differential treatment of Adblocker Users — Jan ’25

Ritik Roongta, Mitchell Zhou, Ben Stock and Rachel Greenstadt *USENIX (to be submitted)*

- Measured the number of **web breakages** caused by adblockers on a pool of 10k websites
- Proposed a taxonomy of invisible and visible breakages and designed tools to measure them independently
- Enhanced Google Chrome’s V8 engine to collect JavaScript execution logs, enabling detection of **malicious patterns** and contributing to improved browser security

A User-Focused Evaluation of Privacy-Preserving Browser Extensions — July ’24

Ritik Roongta and Rachel Greenstadt *AsiaCCS*

- Built a usability and privacy taxonomy from web store reviews to identify user concerns around privacy-preserving browser extensions
- Fine-tuned a Hugging Face **BERT sentiment classifier** to sieve out critical reviews improving accuracy of various **NLP** techniques like LDA and topic modeling
- Devised **11** metrics for evaluating the extensions on performance, permission abuse, web compatibility, etc.

Analysis of web breakages caused by adblockers — May ’24

Ritik Roongta, Mitchell Zhou, Ben Stock and Rachel Greenstadt *SecWeb, S&P*

- Identified **5** major categories of web breakages and conducted web measurement experiments to quantify them
- Implemented advanced crawling techniques to counter server/client-side randomness for deterministic results
- Deployed dynamic code analysis on different websites to detect differential treatment of adblocker users

Drifuzz: Harvesting Bugs in Device Drivers from Golden Seeds — Aug. ’22

Zekun Shen, Ritik Roongta, and Brendan Dolan-Gavitt *USENIX*

- Implemented a framework for concolic fuzzing PCI device drivers (e.g., network interface card)
- Discovered and patched **12 bugs** and obtained **2 CVEs** in the Linux driver code
- Designed test-beds using deprecated versions of linux to compare with legacy softwares like Agamotto

Internship Experience

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
- Instrumented the Google Chrome's V8 engine to collect JS execution logs and visualized them using Python-based scripts
- Conducted in-depth manual analysis of execution logs to detect patterns of **anomalous website behavior**

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
- Interleaved the Linux Kernel with (**AFL**) using kernel driver modules and network programs
- Created a pool of **10,000+** Debian network packages for testing, finding vulnerabilities and reporting **CVEs**

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 placing orders at the exchange
- Processed the BSE and NSE exchange **order-book** with a daily **traffic** in excess of **4 crores** orders and analysed the order delays to develop **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)
- Prepared a detailed documentation covering attacks and mitigation techniques on **OWASP** Top 10 Attacks **2017** (Open Web Application Security Project) along with their video **POCs** (proof of concept)

Reviewer Duties

Program Committee: NDSS '25, PETS '24
Artifact Committee: CCS '24/25, USEMIX '23/24, PETS '25

Technical Skills

Machine Learning: NLP, Computer Vision, Prompt Engineering
Languages: C/C++, Python, Bash, Java, Assembly, JavaScript
Software tools: Puppeteer, Selenium, Git, MATLAB, MySQL, AutoCAD, CMake, LaTeX, AWS
Pentesting: Kali Linux, Metasploit Framework, Xerosploit, Reversing Tools

Awards / Leadership

- Mentored a class of over 100 students in a remote setup for the **Application Security** Course [2022]
- Secured All India Rank **48** in **JEE-Advanced** out of 220,000 shortlisted candidates [2017]
- Awarded **Pratibha Scholarship** for exceptional academic excellence by the Aditya Birla Group [2017-21]
- Awarded **KVPY** Fellowship and **NTSE** Scholarship by the Government of India [2016]