Vijay Prakash

PhD Candidate · ECE

New York University, 370 Jay St., Brooklyn, NY, 11201

✉ vijay.prakash@nyu.edu | 🏠 https://viz-prakash.github.io/ | Google Scholar

Research Overview

My research focuses on responsible and human-centered AI, where I reduce end-user security, privacy, and safety risks in LLMs. Using empirical methods, I uncover risks in generative AI applications and design interventions that address these failures. My work contributes to safer AI systems and offers evidence-based insights for policy and practice.

Education

New York University *Brooklyn, NY, 11201*
PhD ECE *Sep 2021 - present*
- Advisor: Prof. Danny Yuxing Huang

University of Florida *Gainesville, Florida*
MS Computer Science *May 2018*
- Graduate Certificate in Information Security

Savitribai Phule Pune University *Pune, India*
BE Information Technology *May 2014*

Research Experience

08-2022 - Now **Research Assistant, NYU mLab**, New York University

Publications

Ongoing Work

Responsibly Assisting Technology-Facilitated Abuse Survivor Support Ecosystem Stakeholders with Generative AI
Vijay Prakash, Majed Almansoori, Maddy Wu, Rahul Chatterjee, Danny Huang

Published

Assessment of LLMs in the Domain of Technology-Facilitated Abuse
Vijay Prakash, Majed Almansoori, Donghan Hu, Rahul Chatterjee, Danny Huang
Accepted at USENIX Security 2026

Assessment of LLM Responses to End-user Security Questions
Vijay Prakash, Kevin Lee, Arkaprabha Bhattacharya, Danny Yuxing Huang, Jessica Staddon
Proceedings of the 39th Annual Computer Security Applications Conference (ACSAC), 2025

Can Allowlists Capture the Variability of Home IoT Device Network Behavior?
Weijia He, Kevin Bryson, Ricardo Calderon, **Vijay Prakash**, Nick Feamster, Danny Yuxing Huang, Blase Ur
European Symposium on Security and Privacy (EuroS&P), 2024

In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes
Aniketh Girish, Tianrui Hu, **Vijay Prakash**, Daniel J. Dubois, Srdjan Matic, Danny Yuxing Huang, Serge Egelman, Joel Reardon, Juan Tapiador, David Choffnes, Narseo Vallina-Rodriguez
ACM Internet Measurement Conference (IMC), 2023

Behind the Scenes: Uncovering TLS and Server Certificate Practice of IoT Device Vendors in the Wild
Hongying Dong, Hao Shu, **Vijay Prakash**, Yizhe Zhang, Muhammad Talha Paracha, David Choffnes, Santiago Torres-Arias, Danny Yuxing Huang, Yixin Sun
ACM Internet Measurement Conference (IMC), 2023

Inferring Software Update Practices on Smart Home IoT Devices Through User Agent Analysis
Vijay Prakash, Sicheng Xie, and Danny Yuxing Huang
ACM CCS Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses (SCORED), 2022

Examining DES-based Cipher Suite Support within the TLS Ecosystem
Vanessa Frost, Dave (Jing) Tian, Christie Ruales, **Vijay Prakash**, Patrick Traynor, and Kevin R. B. Butler
Asia Conference on Computer and Communications Security (Asia CCS) 2019

Awards, Fellowships, & Grants

2021-2022	**School of Engineering Fellowship**, ECE Depratment, NYU
2016-2018	**Achievement Award Scholarship for New Engineering Graduate Students**, CISE, UF
2017	**SwampHacks 2017 Winner**, The Agency/Gainesville Dev Academy
2013-2014	**Best Senior Year Project in College**, AIT, Pune

Speaking

Learned, Lagged, LLM-splained: LLM Responses to End User Security Questions
ACSAC, Dec 2025

Experimental Aspects of Evaluation of LLM Responses to End-user Security Questions
LASER workshop cohosted at ACSAC, Dec 2025

End-user Security, Privacy, and Safety Risks in Large Language Models
Security Seminar, Cornell-Tech, Nov 2025

In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes
ACM Internet Measurement Conference (IMC), Oct 2023

Inferring Software Update Practices on Smart Home IoT Devices Through User Agent Analysis
SCORED workshop cohosted at ACM CCS, Nov 2022

Teaching Experience

Fall 2025	**Big Data - Grad-level**, Guest Lecture	*CUSP, NYU*
Spring 2025	**Network Security - Grad-level**, Guest Lecture on Intro to Cryptography	*ECE, NYU*
Fall 2023	**Network Security - Grad-level**, Guest Lecture on Intro to Cryptography	*ECE, NYU*
Fall 2023	**Network Security - Grad-level**, Designed and Graded Exam and Assignment	*ECE, NYU*
Fall 2022	**Network Security - Grad-level**, Guest Lecture on Intro to Cryptography	*ECE, NYU*

Industry Experience

JP Morgan Chase *New York, NY*
Summer Associate *Jun - Sep 2023 & 2024*
*AI Research Group: **Hosted by Prof. Jessica Staddon**, and **Dr. Kevin Lee***

- Evaluation of LLMs for end-user security

Palo Alto Networks *Santa Clara, CA*
Senior Security Researcher *May 2018 - Aug 2021*
Security Research Group

- Performed vulnerability research on software used in IoT devices, including Android and ARM Mbed BLE stacks
- Discovered vulnerabilities, including CVE-2021-0968 in the Android Bluetooth stack and CVE-2020-1999 in PAN-OS
- Collaborated on a prototype that fingerprints JavaScript obfuscation using a deep neural network (DNN)
- Built **TCPsession**, a library that extracts JavaScript from HTTP traffic in PCAPs 50× faster than Wireshark
- Improved next-generation firewall capabilities by analyzing vulnerabilities and developing detection signatures

Lastline (now VMware) *Goleta, CA*
Software Engineer Intern *Aug 2017 - Nov 2017*
Anti-Malware Group

- Collaborated to build a prototype classifier to detect PE (Windows executable) malware for inline IPS

Amazon *Seattle, WA*
SDE Intern *May 2017 - Jul 2017*
AWS Perimeter Protection Team

- Built an integration testing framework in Python for AWS Anti-DDoS/WAF product

GS Labs *Pune, MH, India*
SOFTWARE ENGINEER *Jul 2014 - Jul 2016*
Cloud Security

- Lead developer of integrity checking module for Linux OS, Windows OS, and Docker images
- Rewrote the module to fix stability and performance issues for Linux
- Designed and developed the support for Windows and Docker images

Professional Service

PROGRAM COMMITTEE

2026 **Workshop on Technology and Consumer Protection (ConPro)**,

REVIEWER (CONFERENCES)

2026 **The ACM CHI conference on Human Factors in Computing Systems**, **External Reviewer**
2026 **The ACM CHI conference on Human Factors in Computing Systems**, **External Reviewer**
2025 **USENIX Security Symposium**, **External Reviewer**
2025 **The ACM International Conference on AI in Finance (ICAIF)**, **Reviewer**
2024 **USENIX Security Symposium**, **External Reviewer**
2023 **IEEE Symposium on Security and Privacy**, **External Reviewer**
2023 **USENIX Security Symposium**, **External Reviewer**

OTHER SERVICES

2022, 2023 **Center for Cyber Security CSAW Applied Research Competition**, **Student Organizer**
2018, 2019 **SwampCTF**, **Organizing Committee**

SELECTED MEDIA COVERAGE

Oct, 2023 **Your smart home devices are spying on you, this report warns**, Coverage of our work *Wired*

Oct, 2023 **'People have no idea': How smart devices spy on us and reveal information about our homes**, Quoted *El País, Spain*

Oct, 2022 **How the EU's proposed IoT cybersecurity law could affect device makers**, Interview *MorningBrew*

COMMON VULNERABILITIES AND EXPOSURES (CVEs)

2021 **CVE-2021-0968**, Fluoride Bluetooth Stack Integer Overflow Memory Corruption *Android*

2020 **CVE-2020-1999**, Threat signatures are evaded by specifically crafted packets *PAN-OS*