Varun Gandhi

Science and Engineering Complex, 4.421
Harvard University, Allston, MA 02134

vgandhi@g.harvard.edu
vargandhi.github.io

Education

Ph.D., Computer Science, Harvard University, Cambridge, MA — Expected 2025

- **Thesis**: Programming Models and Isolation Mechanisms for Secure Remote Computation
- **Committee**: Prof. Stephen Chong (Harvard, Advisor), Prof. Srinivas Devadas (MIT, Co-Advisor), Prof. Margo I. Seltzer (UBC), and Prof. Eddie Kohler (Harvard)

S.M., Computer Science, Harvard University, Cambridge, MA — 2022

- **Minor**: Public Policy, Harvard Kennedy School
- **Thesis**: Rethinking Isolation Mechanisms for Datacenter Multitenancy

M.Phil., Computer Science, University of Cambridge, Cambridge, UK — 2015

- **Thesis**: Mitigating OpenSSL Attacks in Mobile Devices
- **Committee**: Prof. Alastair R. Beresford and Prof. Ross J. Anderson

B.S., Computer Science, IIIT-Delhi, New Delhi, India — 2013

- Dean's Scholar
- Undergraduate Student Visitor, Carnegie Mellon University, Pittsburgh, PA

Current Research

My research is at the intersection of systems, computer architecture, and security, broadly centered around the design and application of hardware-enforced isolation mechanisms and programming models for verifiable computation to support secure multi-tenancy for datacenter workloads.

Varun Gandhi, Simon Langowski, Stephen Chong, and Srinivas Devadas.
"Rethinking Runtime Integrity Guarantees in Distributed AI Frameworks." In Progress

Varun Gandhi, Stephen Chong, and Srinivas Devadas.
"Privacy Verification in AI workloads." In Progress

Selected Publications and Patents

Stefan Saroiu, **Varun Gandhi**, Alaistair Wolman, and Landon Prentice Cox.
"Liveness guarantees in secure enclaves using health tickets." **U.S. Patent 12,067,111**. August 20, 2024

Stefan Saroiu, **Varun Gandhi**, Alaistair Wolman, and Landon Prentice Cox.
"Automated recovery of far edge computing infrastructure in a 5g network." **U.S. Patent 11,900,127**. February 13, 2024

Varun Gandhi, Sarbartha Banerjee, Aniket Agrawal, Adil Ahmad, Sangho Lee, and Marcus Peinado.
"Rethinking System Audit Architectures for High Event Coverage and Synchronous Log Availability." In 32nd USENIX Security Symposium **(USENIX Security 2023)**

Varun Gandhi, and James Mickens.
"Rethinking Isolation Mechanisms for Datacenter Multitenancy." In 12th USENIX Workshop on Hot Topics in Cloud Computing **(HotCloud 2020)**

Contributions Acknowledged

Alessandro Acquisti, Ralph Gross, and Fred Stuzman.
"Face recognition and privacy in the age of augmented reality" **Journal of Privacy and Confidentiality,** 2014

Industry Research Positions

Cloud and Infrastructure Security Group, Microsoft Research — *Redmond*, WA, USA
Ph.D. Research Intern — Summer 2022
Mentors: Dr. Sangho Lee and Dr. Marcus Peinado

Intelligent Networked Systems, Microsoft Research — *Redmond*, WA, USA
Ph.D. Research Intern — Summer 2021
Mentors: Dr. Stefan Saroiu and Dr. Alec Wolman

Data Systems Group, Microsoft Research — *Redmond*, WA, USA
Pre-Doctoral Research Fellow — 2016-2017
Mentor: Dr. Philip Bernstein

Teaching Experience

Compilers (CS 153) — Harvard SEAS
Teaching Fellow for Prof. Stephen Chong — Fall 2023

Introduction to Distributed Systems (CS 262) — Harvard SEAS
Teaching Fellow for Prof. James H. Waldo — Spring 2023

Critical Thinking in Data Science (APCOMP 221) — Harvard SEAS
Teaching Fellow for Prof. Michael D. Smith — Spring 2020

Invited Talks

Harvard Programming Languages Seminar, 2024 — *Boston*, MA

32nd USENIX Security Symposium, 2023 — *Anaheim*, CA

Microsoft Research Security Workshop, 2022 — *Redmond*, WA

Microsoft Research Security Workshop, 2021 — *Virtual*

12th Workshop on Hot Topics in Cloud Computing, 2020 — *Virtual*

Awards and Honors

USENIX Student Grant — 2023

Harvard Derek C. Bok Certificate of Distinction in Teaching — 2020

Harvard Ralph H. Watson Graduate Science and Engineering Fellowship — 2017

Service and Leadership

Harvard AI Safety Student Team, Technical Member — 2024-2025

Harvard CS-SPYS, Systems Seminar Group, Coordinator — 2024

IEEE Security and Privacy, Shadow PC — 2021

ACM EuroSys, Shadow PC — 2021