Naman Gupta

naman.gupta@pm.me | naman.github.io

Education

University of Wisconsin-Madison, USA Aug, 2021 - Present
PhD in **Computer Science & Engineering** | Minor in Psychology & Gender-Women Studies, Law, and Education

Indraprastha Institute of Information Technology, Delhi, India Aug, 2013 - April, 2017
Bachelor of Technology in **Computer Science & Engineering**

Publications

- Rose Ceccio*, **Naman Gupta***, Majed Almansoori*, and Rahul Chatterjee, "Analyzing Patterns and Behavior of Users When Detecting and Preventing Tech-enabled Stalking". Workshop on Usable Security and Privacy (USEC) **NDSS 2023**.
- Mohannad Alhanahnah, Philipp Schubert, **Naman Gupta**, Thomas Reps, Somesh Jha, and Eric Bodden, "[redacted] Automatic boundary detection in programs". In review at **ICSE 2023**.
- Zhe Tao, Aseem Rastogi, **Naman Gupta**, Kapil Vaswani, and Aditya V. Thakur, "DICE⋆: A Formally Verified Implementation of DICE Measured Boot". **USENIX Security 2021**.
- **Naman Gupta***, Srishti Sengupta* and Vinayak Naik. "A firewall for internet of things.". **COMSNETS, 2017**. *Undergraduate Thesis.*
- **Naman Gupta***, Anmol Singh*, and Sachit Butail. "The effect of instructional priming on postural responses to virtual crowds.". Workshop on Virtual Humans and Crowds in Immersive Environments (VHCIE) **IEEEVR, 2017**.

*equal contribution.

Research Experience

UW Madison, USA August 2021 - Present
Graduate Student, Madison Security & Privacy Group

- Understanding the support seeking process of survivors of Intimate Partner Violence from their social networks.
- Contributed to a novel automatic program splitting algorithm, performed evaluations, and measured its application in software debloating techniques in improving application security.
- Worked on a pipeline to correct natural distribution shifts in a high-dimensional medical imaging dataset using ML-Robustness techniques.

Microsoft Research (MSR), India January 2020 - July 2021
Research Fellow, Confidential Computing Group with Kapil Vaswani

- Implemented a toolchain that runs on commodity hardware to evaluate the formally verified secure boot firmware based on DICE*.
- Performed security evaluation and testing on a Trusted Execution Environment (TEE) architecture on GPUs to find concurrency bugs in the TEE API.
- Implemented an architecture that supports issuance of COVID-19 health certificates & travel permits using Microsoft CCF.

Technology for Emerging Markets Group (Project Blendnet)

- Blendnet is an offline hyper-local video streaming solution to improve financial inclusion for low income population of India.
- Designed to a toolchain for provisioning and configuring the Azure infrastructure.
- Performed preliminary investigation in optimizing the WiFi network for throughput and latency.

IIIT Delhi, India 2013 - 2017
Undergraduate Thesis with Prof. Vinayak Naik

Implemented a prototype architecture that detects security attacks in a home network of IoT devices by intercepting network packets. This study was my first experience with implementing a security-focused research problem.

VR for multi-agent systems with Prof. Sachit Butail

Investigated the viability of a low-cost VR framework to overcome the difficulties of conducting experiments with real crowds, due to stochastic and volatile realistic conditions. In the experiment, the participants witness an interactive VR scene with crowds. We investigate the effect of knowledge priming on the participants by capturing their posture via Microsoft Kinect. This study proved that behavioral contagion can be triggered in VR and it has been used to understand human behavior in a variety of crowd scenarios.

Leadership & Service

- **Best runners-up talk at CS Research Symposium** UW-Madison
- **Teaching Assistant (UW-Madison)** AI (150+) & Programming-III (800+)
- **Teaching Assistant (IIIT-Delhi & NPTEL)** Mobile Computing (200+)
- **Student-Instructor** DSA and System Programming for incoming master's students (50+)
- **Lead, Mentor Program** Paired 200 freshmen with senior students for independent projects
- **Administrator** Software Development Club (conducted several **hackathons**)
- **Talks (sophomore level, 200+)** Virtualization, Security, Git, node.js, MVC frameworks
- **Mentor** Rails Girls Summer of Code
- **Organising Team** 1st Blockchain Summit in India
- **Judge** Google's Code to Learn Contest 2016

Industry Experience

Grab, India | Singapore August 2018 - December 2019
DevSecOps Engineer

- Drove the defensive security initiatives by enforcing hardening policies on the payment infrastructure.
- Evaluated the Docker container security landscape - authorization, seccomp filters, mTLS, and network security groups using SPIFFE.
- Implemented an in-house authentication & authorization workflow for vendor-agnostic Kubernetes with Azure AAD, vulnerability patching, and behavioral monitoring of in-container processes.
- Designed a secret sharing policy in collaboration with the Security Assurance team to vet the security risks involving protocols for third-party vendor secret exchanges.
- Hosted Grab's Security Awareness **CTF with cryptography** challenges.

Media.net (Directi Group), India June 2017 - August 2018
Site Reliability Engineer

- Taught incoming hires (30+) on various topics including systems security, git, virtualization, python, and web framework. Hosted a **systems focused CTF**.
- Migrated a latency-sensitive Java application to a stateless micro-service architecture with monitoring, log collection, and network ingress rules.
- Designed pipeline for a real-time ad-serving platform - a blue-green auto-scaling pipeline (weekly traffic increase of 50%) with 80% reduction in hosting cost and 35% increase in performance.
- Built an automated ticketing system for accountable reporting of infrastructure vulnerabilities.

Intern, Elucidata, India March 2016 - May 2016

- Worked on ElMaven; an data processing engine for large-scale metabolomic experiments enabling faster drug discovery in cancer research.
- The work included optimizing the build system of a large C++ codebase, parallelizing classification algorithms, and solving memory leaks.
- The work is now open-source and the methodology has been published.

Intern, Placement Cell, IIIT-Delhi, India May 2014 - June 2014

- Developed an in-house open-source app for an easy-to-use hiring management experience. The aim was to replace a third-party vendor to safeguard hiring statistics. Gained first-hand experience involving production-grade full-stack development.