Naman Gupta

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

Interests: Systems and Usable Security & Privacy

Education

University of Wisconsin-Madison, USA Aug, 2021 - Present
PhD in **Computer Science & Engineering**

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

Research Experience

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

- Contributed to a novel software debloating technique, performed evaluations and measured it's application in improving application security.
- Currently working on correcting 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
Advisor: 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.

Research Fellow, Technology for Emerging Markets Group (Project Blendnet)
Mentor: Apurv Mehra

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

Publications

- 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.*

  - Implemented a prototype for a firewall on a RaspberryPi to secure the IoT devices in a home-network. The firewall detects different classes of data infiltration attacks on the IoT devices.

  - Implemented a dashboard app for onboarding, allow-listing and displaying metrics about network traffic of IoT devices.
- **Naman Gupta**, Anmol Singh, and Sachit Butail. "The effect of instructional priming on postural responses to virtual crowds.". **IEEEVR, 2017**.

  - Designed a Virtual Reality game by implementing the social force model. The VR game was displayed via a smart phone and VR headset.

  - Conducted between-group experiments to measure knowledge priming on participants wearing the VR headset. We capture the posture movement of the participants through a Microsoft Kinect. (n=26)

  - The results indicate that manipulation of instructions to participants may be used to increase engagement with virtual crowds.

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 worklow for vendor-agnostic Kubernetes with Azure AAD, vulnerability patching and behavioural 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.

Elucidata, India March 2016 - May 2016
Intern

- Worked on ElMaven; an data processing engine for large-scale metabolomic experiments enabling a faster drug discovery in cancer research. The work included optimising 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.

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

- 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.

Responsibilities & Misc.

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

Undergraduate Projects

All the projects listed below are opensourced on Github.

Glowing Hostel PowerDown Challenge Amarjeet Singh
Modeled a 3D interactive online tool using real-time metrics from the smart meters installed in IIIT-Delhi hostels. The model was used to raise awareness and to sensitize students towards electricity wastage.

VR Sculptor, Computer Graphics Ojaswa Sharma
Designed and built a prototype for an application for sculpting objects in AR/VR using a Leap Motion - infrared beam splitter to capture hand skeleton.

Stanford HCI Crowd Research Project, HCI Michael Bernstein

As a member of the Stanford Crowd Research Collective, I performed research on present freelance marketplaces to drive the design of the Open Source platform - Daemo.

SmarTopi, IoT Vinayak Naik

Built a prototype low-cost smart cap (a GoPro + RaspberryPi) that helps the visually impaired persons identify information about their surroundings using image recognition, ML and speech recognition.

Projectile, HCI Ponnurangam Kumaraguru

Built a web-app which connects students and professors, having common interests, to collaborate on academic projects. The project was designed using principles of HCI.

Gourmet Pados Mein, Mobile Computing Vinayak Naik

Built a prototype for a mobile app that provides an opportunity for home cooks and small restaurants to advertise their business, helping people socialize over food.