NAMAN GUPTA

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

Dept. of Computer Science
1210 W Dayton St, Madison, WI 53706

Research Interests: Secure Systems, Privacy, and social aspects of cybersecurity

EDUCATION

PhD University of Wisconsin-Madison, USA — 2021 – *Present*
Computer Science
Advisor: Prof. Somesh Jha

BTech Indraprastha Institute of Information Technology, Delhi, India — 2013 - 2017
Computer Science and Engineering
Advisor: Dr. Vinayak Naik

RESEARCH EXPERIENCE

University of Wisconsin-Madison, USA — 2021 to *Present*
Research Assistant,
Advisor: Somesh Jha

Currently working on building robust and secure Software Debloating techniques.

Microsoft Research (MSR), India — 2020 to 2021
Research Fellow, Confidential Computing Group
Advisor: Kapil Vaswani | Collaborators: Aseem Rastogi, Stavros Volos, Satya Lokam, Aditya V. Thakur

- 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)
Advisor: 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 Wi-Fi network for throughput and latency.

Undergraduate Researcher, IIIT-Delhi

Advisor: Vinayak Naik

- Implemented a prototype for a firewall on a Raspberry Pi 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.

Undergraduate Researcher, IIIT-Delhi
Advisor: Sachit Butail

- Designed a Virtual Reality game by implementing the social force model. The VR game was being 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.

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, S. Sengupta and Vinayak Naik. *"A firewall for internet of things"*. COMSNETS, 2017 and Undergraduate Thesis.

Naman Gupta, A. Singh, and Sachit Butail. *"The effect of instructional priming on postural responses to virtual crowds"*. IEEE Virtual Humans and Crowds for Immersive Environments (VHCIE), IEEEVR, 2017.

INDUSTRY EXPERIENCE

Grab, India | Singapore 2018 to 2019
DevSecOps Engineer

- Drove the defensive security initiatives by enforcing hardening policies on the payment infrastructure.
- Conducted literature review and evaluated key security aspects of the container security landscape - authorization, seccomp filters, mTLS and network security groups using SPIFFE.
- Implemented 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 2017 to 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.

INTERNSHIPS

Elucidata, India 2016
Summer Intern

Worked on ElMaven: a data processing engine for large-scale metabolomic experiments enabling a 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 opensource and the methodology has been published.

IIIT-Delhi, India 2014
Summer 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.

COMMUNITY SERVICE

Glowing Hostel PowerDown Challenge, **IIIT-Delhi** 2013

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.

RESPONSIBILITIES AND MISC.

- **Teaching Assistant (IIIT-Delhi & NPTEL) -** Mobile Computing (200+)
- **Student-Instructor** - DSA & System Programming for incoming master's students (50+)
- **Lead, Mentorship Program -** Paired 200 freshmen with senior students for independent projects Virtualization,
- **Administrator -** Software Development Club (conducted several hackathons)
- **Talks** - Security, Git, node.js, MVC frameworks (sophomore level, 200+)
- **Mentor** - Rails Girls Summer of Code

COMPUTER SKILLS

Language: C, C++, Python, Java, Bash, JavaScript
Tools: GNU Toolchain, CMake, ansible, MATLAB, CI/CD, Containers, Kubernetes

Platforms: Django, Android

OTHER

Sports, Critical Theory, Poetry, Music and Hiking

REFERENCES

Dr. Somesh Jha, Professor
University of Wisconsin-Madison

Dr. Kapil Vaswani, Principal Researcher
Microsoft Research, Cambridge

Dr. Vinayak Naik, Professor
Computer Science
BITS Pilani, Goa, India

Dr. Sachit Butail, Assistant Professor
Mechanical Engineering
Northern Illinois University, USA