MEET UDESHI

+1-607-216-5524 m.udeshi@nyu.edu mudeshi.in udiboy1209

Research Interests: embedded systems security, hardware security, machine learning

EDUCTATION

PhD, Electrical and Computer Engineering, NYU Tandon Sep'22 - Present
Advisors: Prof. Farshad Khorrami and Prof. Ramesh Karri

- Research focus on hardware security and embedded systems security
- Member of Control/Robotics Research Lab and Center for Cybersecurity
- CPGA: 3.958 / 4.000

Dual Degree B.Tech + M.Tech, Electrical Engineering, IIT Bombay Jul'14 - Jun'19
Advisor: Prof. Virendra Singh

- Masters thesis focused on hardware security
- Member of Computer Architecture and Dependable Systems Lab
- CGPA: 8.18 / 10.00

PUBLICATIONS

M. Udeshi, P. Krishnamurthy, H. Pearce, R. Karri, F. Khorrami, "REMaQE: Reverse Engineering Math Equations from Executables," in ACM Transactions on Cyber-Physical Systems, 2024

M. Shao*, S. Jancheska*, **M. Udeshi***, B. Dolan-Gavitt*, H. Xi, K. Milner, B. Chen, M. Yin, S. Garg, P. Krishnamurthy, F. Khorrami, R. Karri, M. Shafique, "NYU CTF Bench: A Scalable Open-Source Benchmark Dataset for Evaluating LLMs in Offensive Security," in Neural Information Processing Systems, 2024

M. Udeshi, P. Krishnamurthy, R. Karri, F. Khorrami, "Tamper-Proof Network Traffic Measurements on a NIC for Intrusion Detection," in IEEE Transactions on Network and Service Management, 2024

N. K. Boran, S. Rathore, **M. Udeshi**, V. Singh, "Fine-Grained Scheduling in Heterogeneous-ISA Architectures," in IEEE Computer Architecture Letters, 2020

ACHIEVEMENTS

Awarded the **DAC Young Fellowship** to present a poster at DAC'23

Awarded the **Recognition of Outstanding Contributions** (RoCStar) at Qualcomm

Received a **Gold Medal** in Indian National Physics Olympiad given to top 35 students across the country

Scored **Advanced Performer (AP)** grade in CS101, awarded to top 3 students in a batch of 200

RESEARCH & WORK EXPERIENCE

PhD Project - Reverse Engineering Math Equations Aug'22 - Present
Control/Robotics Research Lab, Center for Cybersecurity

- Designed REMaQE, an automated framework based on **dynamic analysis** and **symbolic execution** to reverse engineer math equations from binaries
- REMaQE achieves **100% accuracy** in reverse engineering our dataset, with a runtime of **0.48 seconds**
- Designed REMEND, a **neural decompilation** based static analysis framework to reverse engineer math equations from binaries
- REMEND achieves **13.4% higher** accuracy on real-world samples compared to existing neural decompilers

PhD Project - LLM Agents for Cybersecurity Mar'24 - Present
Control/Robotics Research Lab, Center for Cybersecurity

- Compiled the **NYU CTF Bench,** a benchmark of **200 CTF challenges** to evaluate LLM security capabilities
- Developed the **EnIGMA agent** that achieves **13.5%** on NYU CTF Bench

PhD Project - Tamper-Proof Measurements on a NIC Sep'23 - Sep'24
Control/Robotics Research Lab, Center for Cybersecurity

- Designed a framework to collect tamper-proof reliable measurements of high-speed (10GB/s) network traffic on a NIC for intrusion detection on a compromised host
- The framework operates entirely on the NIC, preventing host malware from tampering with network traffic
- Designed a proof-of-concept using SmartNICs and tested the framework for small-scale (10s of connections) to large-scale (1000s of connections) network traffic

Senior Engineer - Qualcomm R&D Bengaluru Jul'19 - Jul'22
ML Compiler Team for Cloud AI100 Accelerator

- Worked on key aspects of AI100 compiler like multi-core, multi-thread and SIMD parallelization, memory management, graph scheduling and operator fusion
- Innovated various **graph optimization techniques** applicable to 2D and 3D computer vision models, recommendation systems and autonomous driving tasks
- Deployed power efficient object tracking pipeline using **Kernelized Correlation Filters (KCF)** on AI100

Master's Thesis - Hardware Security Aug'18 - Jun'19
Guide: Prof. Virendra Singh, CADSL, IIT Bombay

- Designed a **prefetcher disabling attack** to amplify cache side-channel leakage which achieves **99%** reduction in prefetches generated by **AES program**
- Simulated a timing attack on the **re-order buffer** using **SNIPER** x86 simulator
- Implemented **microbenchmarking tools in x86 assembly** to reverse-engineer cache information of Intel cores

R&D Project - HIDC: Heterogeneous-ISA Dynamic Core Aug'17 - Jul'18
Guide: Prof. Virendra Singh, CADSL, IIT Bombay

- Implemented abstractions which help programs running on HIDC to migrate between two ISAs during execution
- Proposed a granular function level migration strategy to reduce cost of migration by **100x**

Google Summer of Code - Kivy May'16 - Aug'16
Python Native UI Framework Game Engine

- Created a **Python+Cython** module for Tiled maps integration with the **KivEnt** Game Engine
- Implemented Cython optimized **Animation System** using entity-component architecture

Software Development Intern - Amazon India Jul'17 - Aug'17
Transportation Financial Systems

- Implemented processing and sorting of **1 million+ receipts** daily using **DynamoDB, SQS**
- Automated server setup containing 30+ AWS resources in **CloudFormation**

SKILLS

Relevant Courses

Hardware Security and Trust
Advanced Computer Architecture
Advanced Hardware Design
Deep Learning

Programming

Embedded C/C++	★★★★★
Python	★★★★★
VHDL/Verilog	★★★★☆

Frameworks

Angr Symbolic Execution	★★★★★
Pytorch Glow Compiler	★★★★☆
LLVM Compiler	★★★★☆
OpenCV	★★★☆☆

Tools and Simulators

Ghidra	★★★★★
Vivado HLS	★★★★☆
Gem5	★★★★☆

OPEN SOURCE CONTRIBUTIONS

Created and maintained **Youtube Fast Playlist**, a webapp to rapidly form playlists from Youtube videos

Contributed the "merge albums" feature to the **beets** music library manager

Collected a bug bounty on bug fixes for the **Kivy Python NUI** framework

Worked on UI aspects of the **wptview** web application for **Mozilla**

Made minor contributions to the **Numpy** repository

LEADERSHIP & TEACHING POSITIONS

Mentor for a hardware security project in the Qualcomm Innovation Fellowship from Aug'20 to May'21

Teaching Assistant for VLSI Design lab in Spring'19 under Prof. Sachin Patkar

Teaching Assistant for Microprocessors course in Fall'18 under Prof. Virendra Singh

Manager of Electronics Club, IIT Bombay for Fall'16 and Spring'17 semesters

Teaching Assistant for Computer Programming flipped classroom in Summer'16 under Prof. D.B.Phatak

Reviewer in the 46th International Physics Olympiad in Jun'15

ACADEMIC PROJECTS

Zedroid: Android on Zedboard — Spring'18

VLSI Design lab, Guide: Prof. Sachin Patkar

- Rebuilt Android 5.0 OS on top of Linux Kernel v3.2 for Zynq platform
- Modified OS init procedure to enable on-board networking with **Android Debug Bridge**
- Interfaced with on-board FPGA for performance intensive applications like video-streaming

Hexapod Navigation using Local Positioning — Spring'18

Embedded Systems course, Guide: Prof. Kavi Arya

- Achieved **10% location accuracy** in $2.25m^2$ area with **RSSI trilateration** for local positioning using **ZigBee**
- Designed a Hexapod with 18 degrees of freedom and implemented path-following robot using local positioning

EXTRA CURRICULARS

Volunteered to teach Business Studies as part of Supplemental Learning Program of **Vidya NGO**

Won third place in Case-Study competition at **Inter-IIT Tech Meet 2018** held at IIT Madras

Awarded **Tech Special Mention** by hostel for year 2015–2016 among 500+ students

Mentored 5 participants in **Kharagpur Winter of Code** to contribute to Youtube Fast Playlist