Suha Sabi Hussain

Website: sshussain.me | Email: suhashussain1@gmail.com | GitHub: suhacker1

Education

Georgia Institute of Technology Aug. 2019 - Aug. 2022
Bachelor of Science in Computer Science (Honors Program) *Atlanta, GA*

- Emphasis on theoretical computer science and human-computer interaction (Threads in People and Theory)
- Relevant Coursework: Intro to Microelectronics and Nanotechnology; Privacy, Technology, Policy, Law

Experience

Security Engineering Intern May 2020 – Present
Trail of Bits *New York, NY*

- Created and maintained a privacy testing library for deep learning written in Python
- Presented at Empire Hacking, OpenMined PriCon, and the DEF CON AI Village Journal Club
- Contributed to the analysis of several vulnerabilities in a cryptocurrecny based on zero knowledge proofs

Research Assistant - Security and Privacy Aug. 2019 – May 2020
Institute for Information Security and Privacy at Georgia Tech *Atlanta, GA*

- Developed data analysis procedures for time-series data to investigate the behavior of a security API
- Researched and curated relevant cases of Internet censorship and surveillance for threat modeling

Cryptography Engineering Intern Dec. 2019 – Jan. 2020
Trail of Bits *New York, NY*

- Contributed to the analysis of a cryptographic privacy vulnerability in a popular security API
- Built a web crawler, NLP classifier, and threat dataset for the simulation of a scenario involving surveillance states

Research Intern - Security and Privacy June 2017 – June 2019
New York University Center for Cybersecurity *Brooklyn, NY*

- Designed a machine learning classifier for privacy violation detection on Android based upon hardware data
- Discovered and instrumented a new method for the exploitation of speech recognition systems
- Presented research to the NSA Board of Directors, NSA Research Directorate, and at the DoD C3E Workshop
- Published in IEEE TIFS. Received awards from the US Navy, ACM, Intel, GoDaddy, NSA, and other groups

Hardware Engineering Intern June 2016 – Aug. 2016
Vengo Labs *Long Island City, NY*

Involvement

Robotics Engineer Aug. 2019 – Present
RoboJackets RoboNav Team *Atlanta, GA*

- Redesigned and deployed a semantic segmentation neural network for an autonomous vehicle
- Design emulators and developer tools for ARM Mbed. Integrate unit testing and fuzzing into firmware

Certifications

Google igniteCS Bootcamp at Columbia University: Mathematical Modeling and Data Science, 2018

Publications & Presentations

S. Hussain,"PrivacyRaven: Comprehensive Privacy Testing for Deep Learning", OpenMined Privacy Conference, 2020.
K. Basu, **S. Hussain**, U. Gupta, and R. Karri, "COPPTCHA: COPPA Tracking by Checking Hardware-Level Activity," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3213–3226, 2020.
S. Hussain, Z. Ghodsi, and R. Karri, "A New Method for the Exploitation of Speech Recogniton Systems," Computational Cybersecurity in Compromised Environments Workshop, 2018.

Technical Skills

General: Software Security, Trustworthy Machine Learning, Deep Learning, Privacy Enhancing Technologies, Applied Cryptography, Program Analysis, Fuzzing, Technical Writing, Probability and Statistics
Languages: Python, C, C++, ARM Assembly, Java, Go, Rust, Bash, LaTeX
Machine Learning: PyTorch, TensorFlow, NumPy, SciPy, Scikit-Learn, Pandas, Matplotlib, PyTorch Lightning
Hardware & Firmware: EagleCAD, Mbed OS, QEMU, AutoCAD, ARM Developer Tools, Arduino