Suha Sabi Hussain

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

Education

Georgia Institute of Technology Aug. 2019 - May 2023
Bachelor of Science in Computer Science (Honors Program) *Atlanta, GA*

- Emphasis on theoretical computer science and human-computer interaction (Threads in Theory and People)
- Relevant Coursework: Privacy: Technology, Policy, and Law; Human-Centered User Interface Design

Experience

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

- Led the development of PrivacyRaven, a privacy testing library for deep learning written in Python. This included implementing novel machine learning attacks, developing robust property-based tests, and meeting with users
- Conducted white-box security audits using manual review, static analysis, and dynamic analysis tools
- Built and contributed to multiple custom open-source tools for machine learning assurance, including fickling
- Identified cryptographic privacy defects in a popular online blocklist API using formal modeling tools
- Participated in and helped organize reading groups on ML, formal methods, program analysis, and cryptography

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

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
- Research was published, presented at multiple venues, and recognized by the NSA, Navy, Intel, ACM, and others

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

Involvement

Program Committee: DEF CON 29 AI Village (August 2021)
Robotics Engineer: Georgia Tech RoboJackets RoboNav Team (August 2019 - October 2020)

Certificates

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

Publications & Presentations

S. Hussain et al.,"Never a Dill Moment: Exploiting Machine Learning Pickle Files", DEF CON 29 AI Village, 2021.
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,"Detecting Privacy Violations in Children's Apps Using HPCs", NSA Board of Directors, 2019.
S. Hussain, Z. Ghodsi, "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
Technical Languages: Python, C, C++, ARM Assembly, Java, Go, Rust, Bash, LaTeX
Machine Learning: PyTorch, TensorFlow, NumPy, SciPy, Scikit-Learn, Pandas, Matplotlib, PyTorch Lightning