Skanda Koppula

450 Memorial Drive
Cambridge, MA 02139

skoppula@mit.edu
skoppula.github.io
1.412.259.3123

Massachusetts Institute of Technology
Masters of Engineering, Computer Systems and Security, GPA: 5.0/5.0 *Sept. 2016 - Present*

Massachusetts Institute of Technology
Major: Computer Science and Engineering, BSc, GPA: 4.7/5.0 *Sept. 2013 - June 2016*

Relevant courses: Machine Learning, Computer and Network Security, Compilers, Digital Communications Systems, Computer Systems Engineering, Cryptography, Design and Analysis of Algorithms (Teaching Assistant), Theory of Computation, Computer Architecture, Operating Systems, Computer Networks, Electronics Projects Lab

Projects and Work Experience

Yahoo Login Abuse Team, Software Engineering Intern *June 2016 - Sep. 2016*

- Prototyped production-ready neural network to classify account registration and login events on Yahoo services as spam. Demonstrated a 6% improvement in network's equal error rate from previous system
- Designed and deployed a multi-threaded data feed service to pull data hourly from Facebook ThreatExchange and thirty-one other sources to inform classifier of threat intelligence updates

Embedded Software Lead for MIT Electric Vehicle Team *August 2016 - Present*

- Developed software and hardware tools to eavesdrop on a Controller Area Network and validate messaging specifications
- Responsible for design and development of various software systems: sensor modules, driver interface boards, and battery management system

Low Latency Speech-Based Authentication *May 2015 - Present*
MIT Energy Efficient Circuits Group

- Designed the first set of low-latency protocols for speaker authentication that prevent memory-snooping attacks. Constructed a software prototype in Scala. Paper in progress.

Square Security Infrastructure Team, Software Engineering Intern *June 2015 - Aug. 2015*

- Modified embedded program to capture memory dump when the Square card-reader crashes
- Developed back-end service to symbolify binary contents to human-readable source error trace

Power-Based Side-Channel Attack for AES Key Extraction *Oct. 2015 - Nov. 2015*
6.858 Final Project - Computer Systems Security

- Built hardware setup to measure power consumption, and implemented the Correlation Power Analysis algorithm. Successfully extracted an AES secret from an Arduino's flash memory measuring only power consumption

Skills

Web Systems: **JAX-RS/Jetty**, **Rails/RSpec**, **Flask**, **JavaScript**
Embedded Systems: **C**, **x86 Assembly** and **Bluespec Verilog**.
Misc: **Python**, **Scala**, **shell**, **Hadoop FS/Hive**, **Spark**, **scipy**, **TensorFlow**

Awards

Analog Devices Research and Innovation Scholar Award	2015
Third Place in Jane Street Collegiate Programmatic Trading Competition	2015
Crowd Favorite Research Poster at the 2016 MIT EECS Research Conference (EECSCon)	2016
Google Science Fair Finalist	2011