Title: Building Trustworthy Computing Systems: From Hardware to Machine Learning and Back

Abstract:

How can users trust that their everyday computing platforms, CPUs, GPUs and ASICs, are performing computations privately and correctly? Indeed, users have good reason to skeptical of the trustworthiness of existing computing systems. For one, most computing hardware is increasingly manufactured off-shore at one of only a few advanced semiconductor foundries. Malicious foundries might pirate and black-market a chip, or potentially even modify its functionality (i.e., insert a hardware Trojan). The first part of this talk will cover my work on how chips can be securely fabricated at untrusted off-shore foundries; the hope is to reap the benefits of advanced manufacturing technology (which might only be available off-shore) without compromising trust.

Another reason for skepticism is the move towards edge and cloud computing. Increasingly, expensive computations are outsourced to (a potentially untrusted) cloud, and particularly so with modern machine learning computations that rely on deep learning. The second part of this talk will cover my work on how outsourced training of deep neural networks introduces new security vulnerabilities, particularly the threat of a backdoored neural network (or BadNets), and how these vulnerabilities can be mitigated. I will conclude by highlighting on-going work in my lab on designing robust and secure deep learning accelerators.

Bio:

Siddharth Garg is an Assistant Professor at New York University in the ECE department. His general research interests are in computer engineering, and more particularly in secure, reliable and energy-efficient computing. For his work, Siddharth has received the NSF CAREER Award (2015), a "Top Picks in Hardware Security" for his NDSS'15 paper, and best paper awards at the IEEE Symposium on Security and Privacy (S&P) 2016, USENIX Security Symposium 2013, NIPS Machine Learning Security Workshop (2017) and the International Symposium on Quality in Electronic Design (ISQED) in 2009. Siddharth also received the Angel G. Jordan Award from ECE department of Carnegie Mellon University for outstanding thesis contributions and service to the community. He serves on the technical program committee of several top conferences in the area of computer engineering and computer hardware, and has served as a reviewer for several IEEE and ACM journals. He received his Ph.D. degree in Electrical and Computer Engineering from Carnegie Mellon University in 2009, an M.S. from Stanford in 2005 and a B.Tech. degree in Electrical Engineering from the Indian Institute of Technology Madras in 2004.