"Towards Hardware Cybersecurity"

Abstract: Designers use third-party intellectual property (IP) cores and outsource various steps in their integrated circuit (IC) design and manufacturing flow. As a result, security vulnerabilities have been emerging, forcing IC designers and end users to re-evaluate their trust in ICs. If an attacker gets hold of an unprotected IC, attacks such as reverse engineering the IC and piracy are possible. Similarly, if an attacker gets hold of an unprotected design, insertion of malicious circuits in the design, and IP piracy are possible.

In this talk I will describe three design for trust techniques that we developed to thwart these and similar attacks: IC camouflaging, logic encryption, and split manufacturing. IC camouflaging modifies the layout of certain gates in the IC to deceive attackers into obtaining an incorrect net list, thereby, preventing reverse engineering by a malicious user. Split manufacturing splits the layout and manufactures different metal layers in two separate foundries to prevent reverse engineering and piracy by a malicious foundry. Logic encryption implements a built-in locking mechanism in ICs to prevent reverse engineering and IP piracy by a malicious foundry and user.

I will conclude the presentation by highlighting why hardware security and trust are important objectives from the economics, security, and safety perspectives and present the vision of this emerging area of hardware cybersecurity.

Bio: Ramesh Karri (http://eeweb.poly.edu/karri/) is a Professor of Electrical and Computer Engineering at Polytechnic Institute of New York University. He has a Ph.D. in Computer Science and Engineering, from the University of California at San Diego. His research interests include trustworthy ICs and processors; High assurance nanoscale IC architectures and systems; VLSI Design and Test; Interaction between security and reliability. He has over 150 journal and conference publications in these areas. He has written two invited articles in IEEE Computer on Trustworthy Hardware, an invited article on Digital Logic Design using Memristors in Proceedings of IEEE and an invited article in IEEE Computer on Reliable Nanoscale Systems.

He was the recipient of the Humoldt Fellowship and the National Science Foundation CAREER Award. He served on the 2006 DARPA ISAT study on “Trust in Integrated Circuits”. He is the area director for cyber security of the NY State Center for Advanced Telecommunications Technologies at NYU-Poly; Hardware security lead of the Center for research in interdisciplinary studies in security and privacy –CRISSP, co-founder of the Trust-Hub and organizes the annual red team blue team event at NYU, the Embedded Systems Challenge.

He cofounded and served as the chair of the IEEE Computer Society Technical Committee on Nanoscale architectures. He is a cofounder and steering committee member of the IEEE/ACM Symposium on Nanoscale Architectures (NANOARCH). He is the Program Chair (2012) and General Chair (2013) of IEEE Symposium on Hardware Oriented Security and Trust (HOST). He is the Program Co-Chair (2012) and General Co-Chair (2013) of IEEE Symposium on Defect and Fault Tolerant Nano VLSI Systems. He is the General Chair of the 2013 NANOARCH. He serves on several program committees. He is the Associate Editor of IEEE Transactions on Information.

Host: Prof. Jakub Szefer, Dept. of Electrical Engineering, Yale University