Indian Institute of Technology Kanpur

INSTITUTE LECTURE SERIES

May 29, 2024 (Wednesday) | 4 pm | L - 17

Talk Title: High-Level Approaches to Hardware and Embedded Security

Speaker: Professor Ramesh Karri

Electrical and Computer Engineering, New York University

About the Speaker

Ramesh Karri is a Professor of Electrical and Computer Engineering at New York University. He co-directs the NYU Center for Cyber Security (http://cyber.nyu.edu). He co-founded the Trust-Hub (http://trust-hub.org) and founded/organizes the Embedded Systems Challenge (https://csaw.engineering.nyu.edu/esc), the annual red-blue team event. Ramesh Karri holds a Ph.D. in Computer Science and Engineering from the University of California at San Diego, and a B.E in ECE from Andhra University. With a focus on hardware cybersecurity, his research and educational endeavors encompass trustworthy ICs, processors, and cyber-physical systems; security-aware computer-aided design, test, verification, validation, and reliability; nano meets security; hardware security competitions, benchmarks, and metrics; biochip security; and additive manufacturing security. Ramesh has published over 300 articles in prestigious journals and conferences. A Fellow of IEEE, Ramesh's work on hardware cybersecurity has earned numerous accolades. He has also received the Humboldt Fellowship and the National Science Foundation CAREER Award. Ramesh is the Editor in Chief of the ACM Journal of Emerging Computing Technologies and an Associate Editor for IEEE and ACM journals. He's had leadership roles in various IEEE conferences and served as an IEEE Computer Society Distinguished Visitor from 2013-2015 and was on the Executive Committee for Security@DAC from 2014-2017.

Abstract of the Talk

As designers increasingly rely on third-party intellectual property (IP) cores and outsourcing in the integrated circuit (IC) design and manufacturing process, security vulnerabilities have been on the rise. This has forced both IC designers and end users to re-evaluate their trust in ICs, as unprotected ICs are susceptible to reverse engineering, IP piracy, and the insertion of malicious circuits and backdoors. In this talk, the speaker will present High-Level Design for Trust techniques that his group has developed to address these threats: Locking of Designs and Secure Sourcing of IPs for High-Level Integration. Implementing built-in locking mechanisms aims to prevent reverse engineering. Secure Sourcing thwarts Trojan insertion in third-party IPs. Dr. Karri will wrap up the presentation by emphasizing the importance of hardware security from economic, security, and safety standpoints, and share his vision for the exciting field of hardware cybersecurity.

All are cordially invited to attend

Office of Dean Research & Development