CAD for (SoC) Security:

Pre-silicon Security Signoff from C to GDSII

Mark Tehranipoor
Intel Charles E. Young Preeminence Endowed Chair Professor in Cybersecurity
Director, Florida Institute for Cybersecurity Research, University of Florida
http://tehranipoor.ece.ufl.edu/ , tehranipoor@ufl.edu

Abstract: SoC security has received significant attention over the past few years. Automation, metrics, standards, and development of computer-aided design (CAD) solutions to provide pre-silicon security vulnerability extraction and countermeasure is still a work in progress. There are numerous security vulnerabilities that must be identified through the course of the design process and addressed before the design is sent for fabrication. Examples include power and EM side channels, fault injection, information leakage, access control, and more. This talk discusses the challenges in developing CAD for SoC security, and presents sample solutions to provide countermeasure at various stages of the design process.

Mark Tehranipoor is currently the Intel Charles E. Young Preeminence Endowed Chair Professor in Cybersecurity at the ECE Department, University of Florida. He is also currently serving as Director for Florida Institute for Cybersecurity Research (FICS), National Microelectronics Security Training Center (MEST), CYAN Center of Excellence, and ECI Transition Center. His current research interests include: IoT security, hardware security and trust, supply chain risk management and security, counterfeit electronics detection and prevention and reliable circuit design. Dr. Tehranipoor has published extensively in the field of hardware security and has delivered more than 200 invited talks and keynote addresses. He has 8 patents, and has published 13 books and 22 book chapters. He is a recipient of 13 best paper awards and nominations, as well as the 2008 IEEE Computer Society (CS) Meritorious Service Award, the 2012 IEEE CS Outstanding Contribution, the 2009 NSF CAREER Award, and the 2014 MURI award. His projects are sponsored by both the industry and Government.

He serves on the program committee of more than a dozen leading conferences and workshops. He served as Program and General Chairs of several leading conferences and workshops. He co-founded a new symposium called IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) and served as HOST-2008 and HOST-2009 General Chair (http://www.hostsymposium.org/). He is currently serving as HOST's Chair of Steering Committee. He is also the co-founder of Trust-Hub (www.trust-hub.org) and Asian HOST (http://asianhost.org/2017/). He serves as co-EIC for newly established Journal on Hardware and Systems Security (HaSS). He also served as an Associate EIC for IEEE Design & Test, an IEEE Distinguished Speaker, and an ACM Distinguished Speaker from 2010 to 2014. He is currently serving as an Associate Editor for JETTA, JOLPE, Transactions on VLSI (TVLSI), and Transactions on Design Automation for Electronic Systems (TODAES). Prior to joining University of Florida, Dr. Tehranipoor served as the founding director of the Center for Hardware Assurance, Security, and Engineering (CHASE) and the Comcast Center of Excellence in Security Innovation (CSI) at the University of Connecticut. Dr. Tehranipoor is a Fellow of IEEE, a Golden Core Member of the IEEE, and Member of ACM and ACM SIGDA. He is currently serving as IEEE Ambassador on Cybersecurity.