CECS
CENTER FOR EMBEDDED & CYBER-PHYSICAL SYSTEMS
UNIVERSITY OF CALIFORNIA · IRVINE

CECS Seminar

"Securing Hardware for Designing Trustworthy Systems"

Prabhat Mishra

Professor of Computer and Information Science and Engineering and a UF Research Foundation Professor at the University of Florida

Tuesday, August 2nd
2:00-3:00 p.m. PST
Location: DBH 4011
Zoom Link

Abstract: System-on-Chip (SoC) is the brain behind computing and communication in a wide variety of embedded systems. Reusable hardware Intellectual Property (IP) based SoC design has emerged as a pervasive design practice in the industry to dramatically reduce SoC design and verification cost while meeting aggressive time-to-market constraints. Growing reliance on these pre-verified hardware IPs, often gathered from untrusted third-party vendors, severely affects the security and trustworthiness of computing platforms. It is crucial to evaluate the integrity and trustworthiness of third-party IPs for designing trustworthy systems. In this talk, I will introduce a wide variety of hardware security vulnerabilities, design-for-security solutions, and possible attacks and countermeasures. I will briefly describe how the complementary abilities of simulation-based validation, formal verification as well as side channel analysis can be effectively utilized for comprehensive SoC security and trust validation.

Biography: Prabhat Mishra is a Professor in the Department of Computer and Information Science and Engineering and a UF Research Foundation Professor at the University of Florida. He received his Ph.D. in Computer Science from the University of California at Irvine in 2004. His research interests include embedded and cyber-physical systems, hardware security and trust, energy-aware computing, system-on-chip validation, machine learning, and quantum computing. He has published 8 books, 35 book chapters, and more than 200 research articles in premier international journals and conferences. His research has been recognized by several awards including the NSF CAREER Award, IBM Faculty Award, three best paper awards, and EDAA Outstanding Dissertation Award. He currently serves as an Associate Editor of IEEE Transactions on VLSI Systems and ACM Transactions on Embedded Computing Systems. He is an IEEE Fellow and an ACM Distinguished Scientist.