Temple University
College of Engineering

Fall Seminar Series
Department of Electrical and Computer Engineering
Wednesday, December 6, 2023
Noon – 1:00 PM EST
Zoom: https://temple.zoom.us/j/95985888360

Hardware Security in the Age of AI: From Semiconductor Devices to Architectures

Soheil Salehi, Assistant Professor

Electrical and Computer Engineering, University of Arizona

Abstract: The current state-of-the-art semiconductor industry heavily relies on the globalized fabrication processes and hardware supply-chain model. While this benefits both participants and their global economy, the security of the underlying hardware is compromised due to various emerging hardware security threats such as side-channel attacks, overproduction, hardware trojan insertion, reverse engineering, IP theft, firmware modifications, and counterfeiting. These security threats have become a significant concern due to the rapid increase of IoT devices used in applications such as human health, public transportation, autonomous vehicles, and environmental monitoring. This talk will demonstrate recent efforts in developing novel approaches for securing IoT hardware and firmware supply chain. Furthermore, this talk will discuss future directions to bridge the ongoing research in deep learning and innovative hardware design to increase the security coverage of hardware. Exciting opportunities will be enabled by the development of novel hardware security measures and research of AI, machine learning, and optimization in the context of security.

Biography: Soheil Salehi is an Assistant Professor in the Electrical and Computer Engineering (ECE) Department at the University of Arizona (UofA) and the director of Privacy-preserving, intelligent, and secure computing Lab (Prism Lab). Prior to joining the UofA, Soheil was a Computing Innovation Fellow (CIFellow) sponsored by the National Science Foundation (NSF) in the Accelerated, Secure, and Energy-Efficient Computing Laboratory and the Center for Hardware and Embedded Systems Security and Trust at the University of California, Davis (UC Davis). He received his Ph.D. and M.S. degrees in ECE from the University of Central Florida (UCF) in 2016 and 2020, respectively. He has expertise in the areas of hardware security and IoT supply-chain security as well as applied ML for secure hardware design. Moreover, he has designed novel circuits and architectures for secure and accelerated computing. Thus far, Soheil has published over 40 journal manuscripts and conference proceedings, and his research has received support from NSF.