Title: Securing Hardware against Physical Adversaries with Unlimited Resources

Speaker: Shahin Tajik (WPI)

Abstract: Electronic computing hardware forms the foundation of our information systems and cyberinfrastructure. The threats to the physical security of computer chips and countermeasures have been widely researched. However, with the rise of more modular and complex computing systems, the physical security of the system is threatened by more sophisticated physical attacks mounted by adversaries with virtually unlimited resources. Such attacks exploit the physical layer characteristics of the computing system beyond the integrated circuits (ICs) and, thus, bypass the conventional attack detection and protection mechanisms. In this talk, we first review some of these powerful physical attacks and discuss why conventional countermeasures fail to defend the system. Afterward, we explore the feasibility of building novel schemes at the physical layer of the system for detecting physical attacks using sensors and responding to them using deception and moving target defenses. Finally, we discuss how academia can assist the industry in discovering such physical vulnerabilities and fixing them before real-world adversaries exploit them.

Bio: Dr. Shahin Tajik is an Assistant Professor at the electrical and computer engineering (ECE) department of Worcester Polytechnic Institute (WPI). He is also the technical lead for the tech area Secure Edge Computing at the Northeastern Microelectronics Coalition (NEMC), which is selected as an innovation hub for CHIPS ACT's Microelectronics Commons program. Dr. Tajik received his Ph.D. in Electrical Engineering in 2017 from the working group SECT, a collaboration of the Technical University of Berlin and Deutsche Telekom Innovation Laboratories in Germany. His field of research includes non-invasive and semi-invasive attacks, Physically Unclonable Functions (PUFs), FPGA Security, and tamper detection mechanisms. Over the last decade, he and his collaborators have discovered novel physical side-channel attacks, such as laser voltage probing (LVP), laser logic state imaging (LLSI), and impedance analysis. His ACM CCS'17 paper "On the Power of Optical Contactless Probing: Attacking Bitstream Encryption of FPGAs" was awarded 1st place in the Applied Research Competition of European Cyber Security Awareness Week (CSAW) in 2017. He was also awarded the best hardware demo at IEEE HOST 2020.