Title: Managing Security Trade-offs Against Economics of Chip Design

Keynote Speaker: Serge Leef, Head of Azure for Secure Microelectronics, Microsoft

Abstract:
While achievement of a zero-trust design, implementation and fabrication processes is a great aspirational goal, it is important to recognize that security comes at a cost for ASICs, SoCs, and Heterogeneous Integration Platforms. A nuanced model of the attack surfaces must be considered in the context of intended applications and trade-offs need to be assessed against performance, silicon area and power dissipation. This challenge calls for a fresh look at the design tools, IP management and re-use practices along with examination of new attack surfaces arising when multiple chiplets are integrated on a silicon interposer.

Bio:
Serge Leef is the Head of Azure for Secure Microelectronics at Microsoft working on leveraging cloud computing to enable profound advances in design, implementation, and fabrication of advanced semiconductors. He joined Microsoft after 3.5 years of national service at DARPA's Microsystems Technology Office (MTO) where he managed a $335M portfolio of programs focused on hardware security and the next generation design technologies. His research interests include computer architecture, chip design tools, simulation, synthesis, semiconductor intellectual property (IP), cyber-physical modeling, distributed systems, secure design flows, and supply chain management.
Leef came to DARPA with executive management experience from Mentor, now Siemens EDA, where he was a Vice President of New Ventures, focusing on electronic design automation and security for hardware and software systems. Leef received his Bachelor of Science degree in electrical engineering and Master of Science degree in computer science from Arizona State University.