CECS

CENTER FOR EMBEDDED & CYBER-PHYSICAL SYSTEMS

CECS Seminar Series

Presents

Hardware Security in the Zynq All-Programmable Soc

Dr. Steve Trimberger
Xilinx Research Lab, San Jose, CA

Abstract: FPGAs have grown from a simple logic replacement to fully-programmable SoC, with multi-core CPU subsystems, a broad spectrum of peripherals, hundreds of thousands of gates of programmable logic and high-speed multi-gigabit transceivers. As the complexity of the underlying hardware has grown, so has the value of the applications built in them and the data handled by them. Traditional FPGA bitstream security has been enhanced to address these greater security requirements. This talk presents an overview of hardware security issues and the security features of the Zynq All-Programmable SoC. The secure boot process includes asymmetric and symmetric authentication as well as symmetric encryption to protect software and programmable hardware during programming. During operation the hardware can disable test ports, monitor on-chip power and temperature and detect tampering with configuration data. ARM Trust Zone is integrated through the AXI busses into both the processor and the programmable logic subsystems.

Biography: Dr. Stephen Trimberger holds a M.S. degree in ICS from UCI and a Ph.D. degree from California Institute of Technology. Since 1988, he has been employed at Xilinx, where he is currently Xilinx Fellow heading the Circuits and Architectures Group in Xilinx Research Labs in San Jose, California. He was the technical leader for the XC4000 design automation software, developed a dynamically-reconfigurable multi-context FPGA, led the architecture definition group for the Xilinx XC4000X device families and designed the Xilinx bitstream security functions in the Virtex families of FPGAs. He led the group that developed the first die-stacked 3D FPGA prototype at Xilinx. He has served as Design Methods Chair for the Design Automation Conference, Program Chair and General Chair for the ACM/SIGDA FPGA Symposium and on the technical programs of numerous Workshops and Symposia. He has authored five books and dozens of papers on design automation, FPGA architectures and hardware security. He has more than 220 patents in IC design, FPGA and ASIC architecture, CAE, hardware security and cryptography. His innovations appear today in nearly all commercial FPGA devices. He is a Fellow of the ACM and a Fellow of the IEEE.

Friday, October 2, 2015 - 2:00pm
Donald Bren Hall 4011
Host: Prof. Fadi J. Kurdahi