Graduate Seminar (EEL 6936)
Department of Electrical Engineering
http://ee.eng.usf.edu/Grad_Seminar

Dr. James Plusquellic

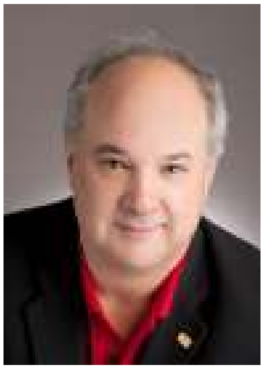
Professor, ECE Department, University of New Mexico
Thursday, November 20, 2014, 1:00-2:00 p.m., CUTR Room 202

Hardware Primitives for Trusted and Secure Systems

Abstract

The increased integration and reliance on remote and embedded electronics as the basis for personal, commercial and military command and control systems is driving the need for improved security and trust in these cyber-physical systems. Subversion of integrated circuits (ICs) in the supply chain is just one recent area of concern, of many, where adversaries can manipulate, sabotage and/or destroy electronic components slated for installation in commercial electronics and critical infrastructures. Capabilities related to the tracking of ICs in the supply chain and for evaluating trustworthiness and security of embedded microprocessors, ASICs, FPGAs, Printed Circuit Boards (PCBs) and other system level components before and after deployment are insufficient to combat the increasing sophistication of intelligent and determined adversaries. An important driver of these types of emerging security and trust problems is globalization. Nearly every step of the modern design process, from architecture, through RTL, layout, manufacturing, packaging, distribution and system integration is 'farmed out' to individual companies located all over the world. This has raised serious concerns over the trustworthiness of components in the supply chain, where substitutions of malicious clones and sub-standard components, are becoming increasingly easier for adversaries because of the lack of component identification information and corresponding tracking mechanisms. Moreover, tools for the evaluation of security and trust, e.g., those that determine whether large complex 3rd party intellectual property (IP) components do what they are supposed to do and nothing more, are non-existent in modern design and test flows. Fundamental changes are required in the IC design flow and authentication processes to combat these vulnerabilities.

In this talk, I will describe several on-chip and PCB-level **security and trust primitives** (**STPs**) that are designed to serve multiple security-related roles including encryption, IC metering (as a countermeasure to over-building) and as side-channel attack detectors, and multiple trust-related roles including authentication, hardware Trojan detection (for the detection of malicious modifications to layouts) and as aging monitors (to combat component 'reuse' in the supply chain). The STPs that we propose are designed to measure basic circuit parameters related to power and delay. Key to the success of using these parameters in security and trust functions is measuring them across the 3-D structure of ICs and PCBs at high resolutions. For example, our proposed techniques make use of stimulus-measure circuits (SMCs) for creating and sensing voltage drops at multiple points in the power distribution system of ICs and PCBs, and a dual-purpose on-chip structure for digitizing voltages (voltage-to-digital converter) and delays (time-to-digital converter). Regional, within-die measurements of power and delay are leveraged in security-related functions, e.g., for implementing **Physical Unclonable Functions** (PUFs), but can also be useful in trust-related functions, e.g., for detecting **hardware Trojan circuits**



Biography

Professor Plusquellic received both his M.S. and Ph.D. degrees in Computer Science from the University of Pittsburgh in 1995 and 1997, respectively. He is currently a Professor in Electrical and Computer Engineering at the University of New Mexico. His research interests are in the area of nano-scale VLSI and include security and trust in IC hardware, silicon validation, design for manufacturability and delay test methods. Dr. Plusquellic received an "Outstanding Contribution Award" from IEEE Computer Society in 2012 for co-founding and for his contributions to the Symposium on Hardware-Oriented Security and Trust (HOST). He served as General Chair for HOST in 2010, for the Defect-Based Testing Workshop in 2006 and is currently serving as Associate Editor for Transactions on Computers. He received the "10 Years of Continuous Service Award" from the International Test Conference, a Best Paper Award from VTS, an ACM Distinguished Service Award from SIGDA and two Austin CAS Fellow Awards from IBM. He recently received a “2014 Innovation Award” from the Science and Technology Center at the University of New Mexico, is a “Featured Entrepreneur” within the School of Engineering and has 3 patents and several provisional applications filed with the U.S. Patent and Trademark Office. Professor Plusquellic is serving or has served on the Program Committees for HOST, Design and Test in Europe, International Test Conference, International Conference on Computer-Aided Design and VLSI Test Symposium. He has published more than 70 refereed conference and journal papers. He is a Golden Core Member of the IEEE Computer Society and a member of the IEEE.