

ECE Seminar

Designing and Fabricating Trusted Hardware in an Untrusted Manufacturing Supply Chain, a Seminar on Hardware Level Attacks and Defenses

Avesta Sasan, Ph.D.

Department of Electrical and Computer Engineering
George Mason University

October 19, 2018, 2:00pm-3:00pm
ENGR 4201

Abstract

Cost of building a new semiconductor fab is estimated to be \$8.0 billion in 2018, with large recurring maintenance costs, a figure that is expected to sharply increase as technology migrates to smaller nodes. To reduce the fabrication cost, and for economic feasibility, most of the manufacturing and fabrication in advanced technology nodes is pushed off U.S. shore. However, many offshore fabrication labs are untrusted. Considering that the hardware is the root of trust in a computing system, this global and untrusted supply chain model has raised concern over potential adversarial attacks with an intimate knowledge of the fabrication process, the ability to modify and expand the design prior to production, and an unavoidable access to the fabricated chips during testing. In this talk, I discuss various trust and security challenges in the untrusted manufacturing supply chain, and provide an overview of the range of defined projects and suggested solutions that my team at GATE laboratory at GMU has been investigating.

Biography

Dr. Sasan received his B.Sc. in Computer Engineering from the University of California Irvine in 2005 with the highest honor (Summa Cum Laude). He then received his M.Sc. and his Ph.D. in Electrical and Computer Engineering from the University of California Irvine in 2006 and 2010 respectively. In 2010, Dr. Sasan joined the Office of CTO in Broadcom Co. working on the physical design and implementation of ARM processors, serving as physical designer, timing signoff specialist, and the lead of signal and power integrity signoff in this team. In 2014 Dr. Sasan was recruited by Qualcomm office of VLSI technology. In this role, Dr. Sasan developed different methodology and in-house EDAs for accurate signoff and analysis of hardened ASIC solutions. Dr. Sasan joined George Mason University in 2016, and he is currently serving as an Associate Professor in the Department of Electrical and Computer Engineering. Dr. Sasan research spans low power design and methodology, hardware security, accelerated computing, approximate computing, near threshold computing, neuromorphic computing, and the Internet of Things (IoT) solutions.