ECE Distinguished Seminar

Is my GPU Secure? Covert and Side Channel Attacks on GPUs

Dr. Nael Abu-Ghazaleh
Computer Science and Engineering Department,
Electrical and Computer Engineering Departments,
University of California, Riverside

Wednesday, April 17, 2019, 11:00 am-12:00 pm
ENGR 4201

Abstract:

Modern computing systems are under attack by increasingly motivated and sophisticated attackers. Recently, the Meltdown and Spectre attacks demonstrated that security is not only a software problem, but that the system hardware components can expose software-exploitable vulnerabilities. With the expanding role of GPUs within computing systems, not only for graphics and multi-media workloads but also as computational accelerators, it is important to understand their security properties. In this talk, I will overview our recent research in understanding covert and side-channel attacks present in modern GPUs. We show that it is possible to construct high bandwidth covert channels, superior in bandwidth and quality to those on GPUs. Furthermore, we show that GPU sharing between multiple workloads also offers opportunities for side channel attacks, and demonstrate several variants of these attacks targeting both graphics and computational workloads. The talk will briefly discuss potential mitigations, and how this type of vulnerabilities is likely to continue to manifest as future computing systems continue to evolve.

Bio:

Nael Abu-Ghazaleh is a Professor in the Computer Science and Engineering as well as the Electrical and Computer Engineering Departments at the University of California, Riverside. He also serves as the chair for the Computer Engineering Program. His research is in architecture support for computer system security, high performance computing, and networked and distributed computing. He has published over 150 papers in these areas, several of which have been recognized with best paper awards or nominations. His hardware security research has resulted in the discovery of several new attacks that have been disclosed to companies including Intel, AMD, ARM, Apple, Microsoft and Nvidia, and received wide coverage from technical news outlets.