ELECTRICAL AND COMPUTER ENGINEERING SEMINAR

Hoda Naghibijouybari
University of California

Security of Graphics Processing Units (GPUs) in Heterogeneous Systems

Thursday, January 30th
138 ISEC
11:45 am – 12:45pm

Abstract:

Graphics Processing Units (GPUs) are integral components to most modern computing devices, used to optimize the performance of today's graphics and multi-media heavy workloads. They are also increasingly integrated on heterogeneous computing servers to accelerate a broad range of applications. Meanwhile, recent trends in security show attacks on modern systems that originate in hardware and are exploitable by software. Given the growing use of GPUs in safety-critical applications, understanding their security properties will become a first-class design objective.

In this talk, I will present my research on covert and side channel attacks and defenses in modern GPUs. I show that it is possible to construct high bandwidth covert channels, superior in bandwidth and quality to those on CPUs. Furthermore, I demonstrate several variants of practical side channel attacks targeting both graphics and computational workloads. The talk will also present architectural mitigations to prevent the discovered attacks. Finally, I will conclude the talk by my planned research at the intersection of emerging architectures and security.

Bio:

Hoda Naghibijouybari is currently a Ph.D. student at the Department of Computer Science and Engineering at the University of California, Riverside. Her research interests include architectural support for security, GPU security, computer architecture and heterogeneous computing. Her research has resulted in the discovery of new attacks that have been disclosed to AMD, and Nvidia companies, and received coverage from technical news outlets. Her paper on GPU Side Channels was one of 11 papers selected for Top Picks in Hardware and Embedded Security, 2019 (identifying best papers in those areas in 2013-2018).