Electrical & Computer Engineering

SEMINAR

Louisiana State University

Cybersecurity from Hardware’s Perspective

Zihao Zhan

Department of Electrical and Computer Engineering

University of Florida

Abstract—In today’s digital era, computer systems are increasingly integrated into our daily lives and industrial operations. In pursuit of computer systems with higher computational performance and energy efficiency, the complexity of computer hardware’s design and implementation has grown significantly. Such complexity, coupled with the intricate interactions between hardware and the physical world, inevitably introduces numerous hardware vulnerabilities. These vulnerabilities not only pose challenges to system security but also highlight the critical need for research focused on identifying and mitigating potential threats originating from hardware vulnerabilities. In this talk, I will present both the attacks exploiting hardware vulnerabilities and the defense strategies against hardware attacks. Specifically, I will detail a side-channel attack that exploits electromagnetic (EM) emanations from GPUs to infer computational activities on GPU and an intentional electromagnetic interference (IEMI) attack that demonstrates the potential for manipulating touchscreen-based devices via externally introduced electric fields. Furthermore, I will introduce a novel defensive technique that leverages EM side-channel information from DRAM to detect and mitigate Rowhammer hardware attacks. Finally, I will outline my future research plans, emphasizing their potential contributions toward advancing the security of future computer systems.

When:	**Wednesday, 6 March 2024, 13:30 - 14:30**
Where:	**Room 3316E Patrick F. Taylor Hall**
Info:	`https://www.lsu.edu/eng/ece/seminar`
Food:	***Coffee, cookies, brownies, etc will be served.***