ELECTRICAL AND
COMPUTER ENGINEERING
SEMINAR

Xiaolin Xu
University of Chicago Illinois

Ensuring Hardware Cybersecurity from a Cross-Layer Perspective

Monday, February 10th

ISEC 138
11:00am-12:00pm

Abstract: The rapid development of the semiconductor industry has significantly increased the number, complexity, and applicability of commercial electronics over the past few decades. As a result, the security and assurance of hardware are playing a critical role in the cyberscape of modern society, such as national defense, healthcare, transportation, and finances. Hardware has been assumed to be trustworthy and reliable “by default.” However, this assumption is no longer true, with an increasing number of attacks reported on the hardware. In practice, the globalization of semiconductor business poses grave risks from untrusted fabrication and distribution, where Trojans insertion, IP cloning, and counterfeits may happen.

In this talk, I will present our research efforts dedicated to the hardware-oriented cybersecurity from a cross-layer perspective. Specifically, I will introduce two frameworks that we built to address these problems in the supply chain and embedded system layers. I will first present an identification technique based on the physical disorder of integrated circuitry that enables the authentication of electronic devices. Then, I will present a hardware IP protection framework based on logic locking and circuit editing, which can effectively mitigate the vulnerabilities from untrusted off-shore foundries and supply chains. At the end of the talk, I will briefly present our scientific achievements in advancing the hardware security in the system and architecture layers, as well as proposing a future research agenda of this emerging area.

Bio: Dr. Xiaolin Xu is currently an Assistant Professor in the Department of Electrical and Computer Engineering at the University of Illinois at Chicago (UIC). Prior to joining UIC, he spent two years at Post-doc Fellow at the Florida Institute for Cybersecurity (FICS) research center at the University of Florida. He received his Ph.D. degree from the University of Massachusetts Amherst in 2016 after he got the B.S. and M.S. degrees in Electrical Engineering from the University of Electronic Science and Technology of China in 2008 and 2011, respectively. His research interests span hardware security and trust, FPGA, IoT security, VLSI, computer architecture, embedded system, and hardware-software co-design for modern computing systems. He is also interested in developing IoT devices and cloud-computing infrastructures with particular emphasis on security, high-performance, privacy protection.