School of EECS Seminar Series Invited Talk

“Hardware Security and Assurance: The Power of Reverse Engineering”

Prof. Domenic Forte
Associate Professor and Steven A. Yatauro Faculty Fellow
Department of Electrical and Computer Engineering, University of Florida

Abstract

Traditional cybersecurity focuses on software and networking and relies on an inherent trust of the underlying hardware. However, the argument that hardware is inherently trustworthy is no longer accurate. The economics of the modern semiconductor industry has created a horizontal supply chain that involves more and more untrusted organizations and IPs. With lesser oversight over supply chains, state level attackers and other hackers can surreptitiously modify integrated circuits (ICs), printed circuit boards (PCBs), and firmware (FW) with hardware Trojans, kill switches, backdoors, and other malware. In addition, e-waste, obsolescence, geopolitical events, and pandemic-related disruptions are incentivizing and facilitating counterfeit electronics.

Hardware assurance refers to activities to ensure a level of confidence that electronics function as intended and are free of known vulnerabilities, either intentionally or unintentionally inserted into a system’s hardware throughout its life cycle. Although reverse engineering is often presented in a negative light, it may be the only foolproof method for providing hardware assurance, especially for commercial-off-the-shelf (COTS) ICs and PCBs where little prior information is available. In this talk, we shall present the recent advances in side-channel based FW reverse engineering as well as IC/PCB reverse engineering steps: delayering, imaging, automated image analysis, and automated annotation. Further, we will delineate the scenarios where reverse engineering can support hardware security and assurance. Finally, we will describe the gaps that need to be filled before realizing the ideal hardware assurance flows.

Oct 29, 2021

11:45 AM - 12:45 PM

Online on MS Teams

Meeting Details

QR CODE for Link

Speaker Bio

Domenic Forte is an Associate Professor and the Steven A. Yatauro Faculty Fellow with the Electrical and Computer Engineering Department at University of Florida. His research covers the domain of hardware security from nano devices to printed circuit boards (PCBs) where he has nearly 200 publications.

Dr. Forte is a senior member of the IEEE, a member of the ACM, and serves on the organizing committees of top conferences in hardware security such as HOST and AsianHOST. He also serves and has served on the technical program committees of DAC, ICCAD, NDSS, ITC, ISTFA, BTAS, and many more.

Dr. Forte is a recipient of the Presidential Early Career Award for Scientists and Engineers (PECASE), the Early Career Award for Scientists and Engineers (ECASE) by Army Research Office (ARO), the NSF Faculty Early Career Development Program (CAREER) Award, and the ARO Young Investigator Award. His research has also been recognized with best paper awards and nominations from IJCB, ISTFA, HOST, DAC, and AHS.