CECS
CENTER FOR EMBEDDED & CYBER-PHYSICAL SYSTEMS
UNIVERSITY OF CALIFORNIA · IRVINE

CECS Seminar

"Anti-virus hardware: Applications in Embedded, Automotive and Power Systems security"

Kanad Basu
Assistant Professor, Department of Electrical and Computer Engineering

Tuesday, June 7th
2:00-3:00 p.m. PST
Location: https://uci.zoom.us/j/97807443602

Abstract: Anti-virus software (AVS) tools are used to detect Malware in a system. However, software-based AVS are vulnerable to attacks. A malicious entity can exploit these vulnerabilities to subvert the AVS. Recently, hardware components such as Hardware Performance Counters (HPC) have been used for Malware detection, in the form of Anti-virus Hardware (AVH). In this talk, we will discuss HPC-based AVHs for improving embedded security and privacy. Furthermore, we will discuss the application of HPCs in security cyber physical systems (CPS), namely automotive and microgrid systems. Subsequently, we will discuss their pitfalls. Finally, we will present PREEMPT, a zero overhead, high-accuracy and low-latency technique to detect Malware by re-purposing the embedded trace buffer (ETB), a debug hardware component available in most modern processors. PREEMPT combines these hardware-level observations with machine learning-based classifiers to preempt Malware before it can cause damage. We will conclude the talk with future research directions and challenges. finding their way to the users.

Biography: Kanad Basu received his Ph.D. from the department of Computer and Information Science and Engineering, University of Florida. His thesis was focused on improving signal observability for post-silicon validation. Post-PhD, Kanad worked in various semiconductor companies like IBM and Synopsys. During his PhD days, Kanad interned at Intel. Currently, Kanad is an Assistant Professor at the Electrical and Computer Engineering Department of the University of Texas at Dallas, where he leads the Trustworthy and Intelligent Embedded Systems (TIES) lab. Prior to this, Kanad was an Assistant Research Professor at the Electrical and Computer Engineering Department of NYU. He has authored 1 book, 2 US patents, 2 book chapters and several peer reviewed journal and conference articles. His research is supported by SRC, NSF, DARPA and Ford Motors. Kanad was awarded the "Best Paper Award" at the International Conference on VLSI Design 2011 and an honorable mention award at the same conference in 2021. Several News agencies have covered his research including NBC Austin and CBS Dallas-Fort Worth. Kanad's current research interests are hardware and systems security as well as Deep learning hardware.