



CECS

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

CECS Seminar

“Dissecting the Software Supply Chain of Modern Industrial Control Systems”



Professor Michail Maniatakos

Associate Professor of Electrical and Computer
Engineering at New York University

Thursday, May 23rd
10:00-11:00 a.m.
Location: Zoom

Abstract:

Recent years have been pivotal in the field of Industrial Control Systems (ICS) security, with a large number of high-profile attacks exposing the lack of a design-for-security initiative in ICS. The evolution of ICS abstracting the control logic to a purely software level hosted on a generic OS, combined with hyperconnectivity and the integration of popular open source libraries providing advanced features, have expanded the ICS attack surface by increasing the entry points and by allowing traditional software vulnerabilities to be repurposed to the ICS domain. In this seminar, we will shed light to the security landscape of modern ICS, dissecting firmware from the dominant vendors and motivating the need of employing appropriate vulnerability assessment tools. We will present methodologies for blackbox fuzzing of modern ICS, both directly using the device and by using the development software. We will then proceed with methodologies on hotpatching, since ICS cannot be easily restarted in order to patch any discovered vulnerabilities. We will demonstrate our proposed methodologies on various critical infrastructure testbeds.

Biography:

Michail (Mihalis) Maniatakos is an Associate Professor of Electrical and Computer Engineering at New York University (NYU) Abu Dhabi, UAE, and a Research Associate Professor at the NYU Tandon School of Engineering, New York, USA. He is the Director of the MoMA Laboratory (nyuad.nyu.edu/momalab), NYU Abu Dhabi. He received his Ph.D. in Electrical Engineering, as well as M.Sc., M.Phil. degrees from Yale University. He also received the B.Sc. and M.Sc. degrees in Computer Science and Embedded Systems, respectively, from the University of Piraeus, Greece. His research interests, funded by industrial partners, the US government, and the UAE government include privacy-preserving computation and industrial control systems security.

Hosted By: Prof. Mohammad Al Faruque