Friday, 1 July 2022, 14:00 - 15:00
Room 105 or via zoom here

KIOS Seminar Series

Prof. Mihalis Maniatakos
New York University (NYU),
Abu Dhabi, UAE

Security evaluation of industrial control systems using system emulation and fuzzing

LECTURE 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, as well as a substantial number of research works that try to proactively uncover underlying vulnerabilities. The main focus on both sides, though, has been the first and obvious choices when it comes to exploitation, namely the network level as the main gateway to an ICS and the control operation performed by it. As ICS evolve abstracting the control logic to a purely software level hosted on a generic OS, software level evaluation of multiple levels of an ICS is a straightforward choice. In this talk, we will motivate the use of system emulation for the cybersecurity assessment of ICS such as Programmable Logic Controllers (PLC) for in-field security evaluation with no disruption to the actual process. More specifically, we will deploy system emulation to eliminate the need for experiments directly on the actual hardware device, massively improve scalability and compatibility for easy deployment on a multitude of platforms. On the emulated platform, we will apply fuzzing across software levels of the device, the system itself, the hosted PLC abstracting platform as well as the application performing the control logic. Through fuzzing we expose vulnerabilities existing on the system either by poor maintenance or sloppy programming. The PLC platform of choice is the Codesys runtime, an industry-leading solution existing in a quarter of the currently deployed PLC.

BRIEF BIO

Mihalis Maniatakos is an Associate Professor of Electrical and Computer Engineering at New York University (NYU) Abu Dhabi, Abu Dhabi, U.A.E., and a Global Network University Associate Professor at the NYU Tandon School of Engineering, New York, NY, USA. He is the Director of the MoMA Laboratory (https://wp.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, New Haven, CT, USA. 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. Prof. Maniatakos has authored several publications in IEEE transactions and conferences, holds patents on privacy-preserving data processing, and also serves in the technical program committee for various international conferences.

The KIOS CoE has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 739551 and the government of the Republic of Cyprus through the Deputy Ministry of Research, Innovation, and Digital Policy. Complementary funding for the KIOS CoE is also provided by the University of Cyprus and Imperial College London.