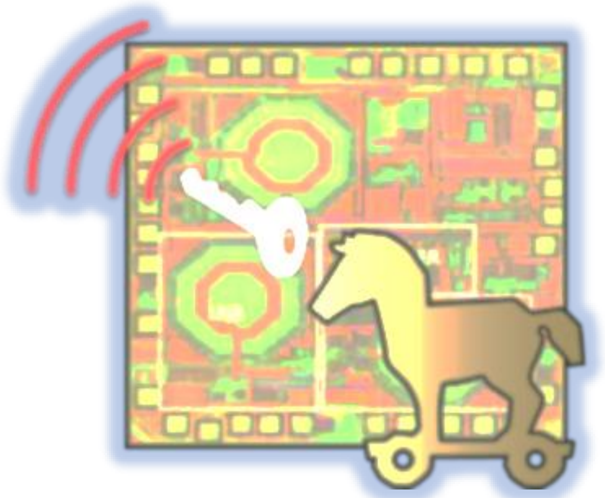

Call for participation

Seasonal School in Cybersecurity:

Critical Infrastructure Security

(Applications deadline: April 30, 2017)

Description: The program consists of 4 2-hour modules focusing on the topic of critical infrastructure cybersecurity. The seasonal school is open to graduate and senior undergraduate students in Computer Science, Computer Engineering, Electrical Engineering, or related fields.

Speaker: Dr. Mihalis Maniatakos, Assistant Professor of Electrical and Computer Engineering, New York University Abu Dhabi nyuad.nyu.edu/momalab

Certificate of attendance: While the lectures are open to the public, a certificate of attendance will be provided given: a) Attendance of all 4 modules, b) Successful completion of assignments (Two assignments will be given: The first will be to create a 20-min Powerpoint presentation on a provided topic, and the second will be a 6-page research report).

Application process: Interested students can apply by sending their most recent CV (max 1 page) and their list of grades to Prof. Alkis Hatzopoulos (alkis@eng.auth.gr) **by April 30th**. Admitted applicants (**up to 15**) will be informed during the first week of May. There are no fees for attending the school.

Content: The seasonal school will consist of 4 modules:

17/5, 12-2 pm: Module 1: Basics of security and privacy, critical infrastructure
19/5, 2-4 pm: Module 2: Security of the power grid. First assignment due 29/5.
29/5, 12-2 pm: Module 3: Industrial control systems security. Second assignment due 5/6.
31/5, 12-2 pm: Module 4: Students' presentations, open discussion.

Detailed description: Cyberattacks on critical infrastructure can have a debilitating effect on national economic security, public health, and safety. The underlying processes of the various critical infrastructure sectors are controlled by Industrial Control Systems (ICS). ICS are transitioning from legacy, electromechanical-based systems to modern information and communication technology-based systems, creating a close coupling between cyber and physical components. This transition greatly expands the attack surface of such systems, as cyberattacks targeting commercial-off-the-shelf hardware and software are well-known. In this series of seminars, we provide an academic perspective to ICS cybersecurity, presenting case studies on cyberattacks and defenses for two critical infrastructure sectors: the power grid and the chemical sector. We also discuss the need for an accurate assessment environment, achieved through the inclusion of Hardware-In-The-Loop testbeds.