Title: Cybersecurity for the smart-grid: Manhattan Case Study

Abstract: Critical infrastructure operations and control systems have become increasingly automated, incorporate two-way communications, and may also be connected to the Internet or other computer networks. While these improvements have allowed for modernization of critical infrastructures, this increased interconnectivity has made the infrastructure more vulnerable to remote cyber-attacks. Cyber-attacks can create instant effects at very low cost, and are very difficult to positively attribute back to the attacker. There are numerous examples of such cyber-attacks, and their rate against corporate and government infrastructure is on the rise and unlikely to abate. A major contributor to the increase of cyber-attacks, is the recent shift to "smart" devices. These devices provide numerous capabilities to the owners, but serve as points of entry to adversaries. In this talk, we will provide a smart-grid case study, discussing the security of typical controllers using a red-team/blue-team approach on a testbed developed at NYU, as well as presenting low-cost intrusion detection methodologies for embedded controllers.

Speaker bio: Michail Maniatakos is a Research Assistant Professor of ECE at New York University Polytechnic School of Engineering at Brooklyn, NY and an Assistant Professor of ECE at New York University Abu Dhabi. Prof. Maniatakos received his Ph.D. from Yale University in 2012, as well as an M.Phil. and M.Sc. in 2009 and 2008 respectively. He has also received a B.Sc. and M.Sc. in Computer Science and Embedded Systems from the University of Piraeus, Greece in 2006 and 2007 respectively. He is the director of the Modern Microprocessor Architectures (MoMA) lab in NYU Abu Dhabi, an IEEE Member and an author of multiple publications in IEEE Transactions and conference papers. He has received a $400K grant from Consolidated Edison, New York, for his work on smart-grid cybersecurity. His research interests include privacy-preserving general-purpose computation, hardware security and industrial control systems security.