UCF | Electrical and Computer Engineering

Spring 2017 Seminar Series

Detection and Prevention of Intrusions in Power Systems' Cyber-Physical Infrastructure

THURSDAY MARCH 30, 2017

11:30 AM – HEC 450

In recent years, adversaries show the high intelligence to perform attacks against cyber-physical systems, such as power grids. They stay stealthily for a long period, learn physics about control systems, and use malicious commands crafted in legitimate formats to cause physical damage. Different from previous work, my research combines the knowledge of both cyber and physical infrastructures to detect the attacks and prevent the damage from happening. I designed network intrusion detection systems that use the physical model of power systems to detect malicious commands and a self-healing network to restore measurements from compromised power grid devices. In my current work, I propose Raincoat, which randomizes data acquisitions to disrupt attackers' knowledge. Meanwhile, we intelligently spoof measurements to mislead attackers into designing ineffective strategies. Based on experiments using large-scale power systems and six real wide area networks, Raincoat is effective against false data injection and control-related attacks with small overhead. At the end of this presentation, I will present my future work that targets different attack model and uses the "big volume of small data" model to increase the resilience design.

Hui Lin

University of Illinois at Urbana-Champaign

Hui Lin earned his B.S. degree from Huazhong University of Science and Technology in 2006 and his M.S. degree from the University of Illinois at Chicago in 2010, both in electrical and computer engineering. He is currently working toward his Ph.D. degree at the University of Illinois at Urbana-Champaign. His research interests include cyber security, intrusion detection systems, and software-defined networking (SDN). His Ph.D. research explores applying intrusion detection systems and SDN in critical cyber-physical systems, such as power grids, to increase their resilience against cyber attacks and accidental failures. He has successfully adapted Bro, a runtime network traffic analyzer, to support network protocols (e.g., DNP3) commonly used in power grid infrastructure. The DNP3 analyzer that he developed has been included in Bro and can be downloaded freely by utility companies. His current work focuses on applying SDN in cyber-physical systems; he intends to use SDN's network programmability to design flexible cyber-physical systems which can preemptively prevent cyber-attacks from introducing physical damage.

.