ITC 2024 Cairo Invited Talk

Advancing Security in Cyber-Physical Systems

Prof. Amr Youssef

Professor, Concordia Institute for Information Systems Engineering,
Concordia University, Canada.
E-mail: amr.youssef@concordia.ca
Web: https://www.concordia.ca/faculty/amr-youssef.html

ABSTRACT

As cyber-physical systems (CPS) continue to evolve, ensuring robust security measures becomes increasingly critical. In this talk, I will present innovative approaches rooted in control theory to address security challenges in CPS environments. I will start by presenting some of our work on the development of Wyner wiretap-like encoding schemes and covert channel techniques, exploiting control logic alterations and robust reachability arguments to establish undetectable communication channels between compromised controllers and eavesdroppers. Then, I will explore key agreement schemes for CPS, leveraging asymmetry in the plant model knowledge available to control system (the defender) and to the eavesdropper, to establish common secret keys without resorting to classical cryptographic methods. Finally, I will address the challenge of verifying control signals received from cloud-based encrypted controllers. I will describe a computationally inexpensive verifiable computing solution inspired by probabilistic cut-and-choose approaches, enabling plant actuators to validate computations without compromising performance.

BIO

Dr. Amr Youssef received the B.Sc. and M.Sc. degrees from Cairo University, Cairo, Egypt, in 1990 and 1993 respectively, and the Ph.D. degree from Queens University, Kingston, ON, Canada, in 1997. Dr. Youssef is currently a professor at the Concordia Institute for Information Systems Engineering (CIISE) at Concordia University, Canada. Before joining CIISE, he worked for Nortel Networks, the Center for Applied Cryptographic Research at the University of Waterloo, IBM, and Cairo University. His research interests include cryptography, cyber-security, and cyber-physical systems security. He has about 300 referred publications in areas related to his research interests. He was the co/chair for Africacrypt 2013 and Africacrypt 2020, the conference Selected Areas in Cryptography (SAC 2014, SAC 2006, and SAC 2001).