INCS-CoE

International Cybersecurity Center of Excellence
https://incs-coe.org

Security Challenges of Next Generation Energy Distribution Networks

Wednesday, June 5, 7:00-8:30 am US EDT / 12:00-1:30 pm UK / 1:00-2:30 pm CET / 2:00-3:30 pm Tel Aviv / 7:00-8:30 pm Perth / 8:00-9:30 pm Japan / 9:00-10:30 pm Canberra

Dirceu Cavendish, Kyushu Institute of Technology, Japan

Bio: Dirceu Cavendish received his bachelor degree in Electronics from Federal University of Pernambuco, Brazil in 1986. He spent five years as a telecommunications engineer in the Business Communications Division of Philips. He received his M. S. in Computer Science from Kyushu Institute of Technology, Japan, in 1994, and his Ph. D. from Computer Science Department-UCLA in 1998. From 1998 to 2006, Dr. Cavendish conducted research in Optical Transport Networks, IP, and Ethernet technologies at NEC Labs America. Since 2007, Dr. Cavendish has been part of the Faculty Staff of Kyushu Institute of Technology. His current research interests include LEO satellite networks, security of medical systems and electrical grids.

Electric Vehicle Authentication and Secure Metering in Smart Grids

Electric vehicles have been recently produced at a very aggressive pace as a way to curb carbon emissions in the 21st century. Public utility companies are rushing to provide electric vehicle charging station infrastructure needed to serve a rapidly growing fleet of EV users in various countries around the world. Equipped with smart meters, charging stations must check vehicle's characteristics prior to charging, as well as securely report charging data back to public utility companies. In this talk, we propose to leverage an Authentication and Key Agreement protocol used in cellular networks into an electric vehicle authentication and secure metering framework. Starting with a vehicle Subscriber Identification Module, we show how generic vehicle services can be securely provided, including mutual authentication, key agreement, and key management issues.

Ali Mehrizi-Sani, Virginia Tech, USA

Bio: Ali Mehrizi-Sani received the Ph.D. degree in electrical engineering from the University of Toronto in 2011. He is currently an Associate Professor with Virginia Tech. He is a Senior Editor for IEEE Transactions on Energy Conversion and is or has been on the editorial board of IEEE Transactions on Power Delivery, IEEE Transactions on Power Systems, IEEE Power Engineering Letters, and IET Generation, Transmission and Distribution. Among his recognitions are the 2018 IEEE PES Outstanding Young Engineer Award and the 2017 IEEE Mac E. Van Valkenburg Early Career Teaching Award. He has over 180 refereed publications.

Renewables and Cybersecurity: Friends or Foes?

Power system is a critical infrastructure whose geographical expanse and pervasive use of information and communication technologies (ICT) make it an attractive target for cyberattacks. Increasing integration of renewables, especially through grid-forming (GFM) inverters, exacerbates this challenge. Compared with other modes of operation, GFM inverters can support a wider host of functionalities leading to a more pronounced impact on the system performance. This complicates the design of their cybersecurity detection and mitigation algorithms as attackers can compromise GFM inverters through different attack types, circumventing the existing cybersecurity approaches that are largely designed for one specific attack type. This talk discusses, at a high level, our work to address this gap via a diverse set of detection and mitigation methods. Specifically, this talk will share our work on physics-informed machine learning—based cybersecurity of control and power sharing algorithms for renewable generation units. This approach is validated using offline and real-time simulation studies on standard test power systems as well as on our digital twin representing the Virginia Tech-owned utility, VTES. At the end, this talk also discusses how the twin problems of the design of the control system and the design its cybersecurity algorithms can be considered as one simultaneous problem.

Fei Teng, Imperial College London, UK

Bio: Fei Teng is the Director of Education at Energy Futures Lab, a pan-university hub promoting inter-disciplinary research in energy, and a Senior Lecturer in the Department of Electrical and Electronic Engineering at Imperial College London. He holds visiting positions at MINES Paris, France, PolyU, Hong Kong and KTH, Sweden. His research primarily focuses on the interplay of energy and digital technologies. He is a leading researcher in software-defined power grids and the cyber resiliency of digitalized power grids.

Cyber Resiliency of Digitalized Power Grids - Keep the Lights on!

The digitalization of the power grid is one of the key components to support a cost-effective transition toward “Net-zero”. However, the increasing cyber-physical dependency causes potential vulnerabilities against cyberattacks that may lead to catastrophic damage to the power grid. It is hence critical to understand such vulnerabilities and develop capabilities to maintain safe operations under those attacks. This talk will present the cyber-resiliency framework and our recent research on cyberattack mitigation and recovery strategies for digitalized power grids.