TEMPLE UNIVERSITY®

\

Fall 2021 Colloquium

Department of Computer and Information Sciences

Trustworthy Critical Infrastructures via Physics-Aware and AI-Powered Software Security

Dr. Saman Zonouz

Associate Professor
Electrical and Computer Engineering Department
Rutgers University

Wednesday, November 10th, 11 AM
https://temple.zoom.us/j/98278541291

Abstract: Critical cyber-physical infrastructures, such as the power grid, integrate networks of computational and physical processes to provide the people across the globe with essential functionalities and services. Protecting these critical infrastructures' security against adversarial parties is a vital necessity because the failure of these systems would have a debilitating impact on economic security and public health and safety. Our research aims at provision of real-world solutions to facilitate the secure and reliable operation of next-generation critical infrastructures and require interdisciplinary research efforts across adaptive systems and network security, cyber-physical systems, and trustworthy real-time detection and response mechanisms. In this talk, I will focus on real past and potential future threats against critical infrastructures and embedded devices, and discuss the challenges in design, implementation, and analysis of security solutions to protect cyber-physical platforms. I will introduce novel classes of working systems that we have developed to overcome these challenges in practice.

Bio: Saman Zonouz is an Associate Professor in the Electrical and Computer Engineering Department at Rutgers University. His research has been awarded by Presidential Early Career Awards for Scientists and Engineers (PECASE) by the United States President in 2019, NSF CAREER Award in 2015, National Security Agency (NSA) Significant Research in Cyber Security in 2015, Google Security Award and Hall of Fame Recognition in 2015, Top-3 Demo at IEEE SmartGridComm 2015, the Faculty Fellowship Award by Air Force Research Laboratory (AFRL) in 2013, the Best Student Paper Award at IEEE SmartGridComm 2013, the University EARLY CAREER Research award in 2012 as well as the Provost Research Award in 2011. The 4N6 research supporters include National Science Foundation (NSF), Department of Homeland Security (DHS), Office of Naval Research (ONR), Department of Energy (DOE), Advanced Research Projects Agency Energy (ARPA-E), Department of Education (DOE), Siemens Research Labs, WinRiver, GrammaTech, Google, ETAP, and Fortinet. Saman has served as the chair, program committee member, guest editor and a reviewer for top international journals and conferences (e.g., IEEE Security and Privacy – Oakland, CCS, NDSS and DSN). Saman served on Editorial Board for IEEE Transactions on Smart Grid, and has been invited to Co-Chair the organization of the National Science Foundation's CPS PI Meeting. He obtained his Ph.D. in Computer Science from the University of Illinois at Urbana-Champaign.