Trustworthy Critical Infrastructures via Physics-Aware Just-Ahead-Of-Time Verification

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 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 and development projects aim 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, and finally conclude with several concrete directions for future research. Additionally, I will briefly go over our other projects on x86 malware/memory analysis and embedded systems security solutions to support access control applications in cyber-physical settings.

Biography: Saman Zonouz is an Assistant Professor in the Electrical and Computer Engineering Department at Rutgers University since September 2014 and the Director of the 4N6 Cyber Security and Forensics Laboratory. His research has been awarded NSF CAREER Award in 2015, National Security Agency (NSA) Significant Research in Cyber Security in 2015, Google Security Award in 2015, Top-3 Demo at IEEE SmartGridComm 2015, the Faculty Fellowship Award by AFOSR 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 Corporation. In addition to research publications, Saman's research efforts have resulted in several tech-to-market transition initiatives such as the founded Kaedago Inc. startup company (as the result of the ARPAE project), a recent startup company (Sekurity LLC) and the Siemens-funded project to adopt his developed controller program analysis algorithms (originally supported by NSF CPS program) for programmable logic controllers (PLCs). Saman's current research focuses on systems security and privacy, trustworthy cyber-physical critical infrastructures and embedded platforms, binary/malware analysis and reverse engineering, as well as adaptive intrusion tolerance architectures. Saman has served as the chair, program committee member, guest editor and a reviewer for top international conferences and journals. Saman serves on Editorial Board for IEEE Transactions on Smart Grid. He obtained his Ph.D. in Computer Science, specifically, intrusion tolerance architectures for the cyber-physical infrastructures, from the University of Illinois at Urbana-Champaign in 2011.