Distinguished Lecture by Prof. Sandeep Shukla, IIT Kanpur

September 30, 2018

Prof. Sandeep Shukla is currently Poonam and Prabhu Goel Chair Professor and Head of Computer Science and Engineering Department at IIT Kanpur. He is Coordinator of the Interdisciplinary Center for Cyber Security and Cyber Defense of Critical Infrastructure at IIT Kanpur. He is Editor-in-Chief of ACM Transactions on Embedded Computing Systems.

His research interests are formal methods, system level design languages and frameworks, component based and platform based design, system level power management, formal verification and its use in system design, embedded system design, software engineering for embedded systems, distributed object technology, networked embedded systems.

Title: Research Issues in Security in Cyber-Physical Systems

Abstract: Cyber Physical Systems are physical systems inextricably entangled with cyber based control – such as power plants, power transmission, distribution systems, water treatment plants, automated manufacturing systems etc. Such systems form the backbone of national wellbeing and are termed as national critical infrastructures. In today's cyber threat landscape, these systems are ripe targets of powerful cyber-attacks from nation states, hackers or cyber criminals. As a result, securing such systems is of paramount importance. Due to their cyber physical nature, the security problems germane to such systems are quite different from that of traditional ICT systems. The attack surfaces range from measurement instrumentation in the physical components, the industrial protocols and networks, the control systems, the actuators, and more depending on the span and functionality of the systems. Cyber-attacks on such systems have happened even for air-gapped facilities as seen in the case of the STUXNET attack on nuclear enrichment plant in Iran. Ukraine power system attacks are prime examples of cyber-attacks on power grid, and Ukraine water chlorination chemical plant attack attempt has been as recent as summer of 2018. How does one prepare for defending these systems? It requires proper risk modeling, malware and intrusion detection through machine learning, continuous surveillance and automated threat detection and prevention, systematic patching through real-time threat intelligence, dynamic adaptive cyber defense through run-time reconfiguration, and many such techniques. Cyber resilient design of such systems is even a better step towards preparedness. Awareness, and education is a significant component of the defense strategy as human computer interaction is more in such systems through human-in-the loop control architectures. In this talk, we present some of these burgeoning fields of cyber security research and discuss how the C3I Center at IIT Kanpur is putting some of these to practice.