Invited Talks

Department of Computer Science and Engineering
Indian Institute of Technology Kanpur
December 29, 2017

Time: 2:30 – 4:30 PM

Venue: RM 101

Talk 1: 2:30 – 3:30

Towards Secure and Privacy-aware Cyber-Physical Systems and IoT

Mani Srivastava, UCLA

mbs@ucla.edu

http://www.ee.ucla.edu/mani-srivastava/

Abstract: Sensors in our phones, sensors on our bodies, sensors in our spaces. Just in a short time span we seem to have been inundated by sensors everywhere. Sitting at the edges of the emerging distributed computing fabric being called the Internet of Things (IoT), networked sensors produce rich data of high volume, velocity, and variety. These sensory data streams enable pervasive awareness, predictive analytics, customization and just-in- time intervention in a variety of application domains such as mHealth, smart buildings, and intelligent transportation.

While their benefits are numerous, sensors also present immense new privacy and security risks that are hard to comprehend as the high-dimensionality sensor data is quite different from other data that we encounter in our lives and have experience with. Sophisticated adversaries, benefiting from the same advances in computing technologies as the sensing systems, can manipulate sensory sources and analyze data in subtle ways to extract sensitive knowledge, cause erroneous inferences, and subvert decisions. The consequences of these compromises will only amplify as our society increasingly complex human-cyber- physical systems with increased reliance on sensory information and real-time decision cycles.

The problems of privacy and security are getting magnified as the early sensing-focused IoT systems are leading to a new generation of IoT systems where the sensor data is being used to influence and control the state of human-cyber-physical systems at multiple scales ranging from personal to societal. The sensor data, instead of being ingested primarily for slower time-scale knowledge discovery and decision making, is becoming part of a complex web of distributed autonomous and semi-autonomous feedback loops controlling and coordinating swarms of autonomous devices owned and managed by multiple parties and intelligently operating in shared spaces while interacting with humans and the physical world around them. Such systems present new threats and system vulnerabilities, such as corruption of control loops, exploitation of physical channels among sensors and actuators, and manipulation of timing information that control algorithms critically depend upon.

Drawing upon examples from applications such as mobile health and sustainable buildings, this talk will discuss the challenges in designing a trustworthy computing substrate for pervasive perception, cognition, and action. For it to be trusted by both, the pervasive sensing infrastructure must be robust to active adversaries who are deceptively extracting private information, manipulating beliefs and subverting control decisions. Solving these challenges would require a new science of resilient, secure and trustworthy networked sensing and control

systems that combines methods from multiple disciplines, and the talk would provide some initial insights and results.

Speaker Bio: Mani Srivastava is on the faculty in the ECE Department at UCLA, with a joint appointment in the CS Department. Previously, he obtained his undergraduate degree from IIT Kanpur, his MS and PhD from UC Berkeley. Before joining UCLA, and worked at Bell Labs Research. His research is broadly in the area of networked human-cyber- physical systems, and spans problems across the entire spectrum of applications, architectures, algorithms, and technologies. His current interests include issues of energy efficiency, privacy and security, data quality, and variability in the context of systems and applications for mHealth and sustainable buildings. He is a Fellow of the ACM and the IEEE. More information about his research is available at his lab's website: http://www.nesl.ucla.edu.