Faculty Candidate Seminar

Safeguarding User Privacy in the CPS energy systems

Dong Chen

University of Massachusetts

Abstract: The rise of the Cyber-Physical Systems (CPS) holds great promise to transform people's lives by making society more efficient in many areas, including energy, transportation, healthcare, manufacturing, etc. At their core, CPS devices use sensors to collect data on real-world physical processes and then transmit it over the Internet to cloud servers, which store, process, and learn from the data to better optimize these processes. Unfortunately, CPS devices also expose users to multiple new types of privacy attacks. In particular, the sensor data collected from CPS devices can indirectly reveal a variety of sensitive private information.

In this talk, I will discuss my recent work on sensor data privacy in the context of Cyber-Physical Energy Systems (e.g., smart grid) to provide examples of the surprising types of private information (e.g., location, occupancy, behavior, appliance energy signatures etc.) that I can glean from seemingly innocuous CPS data. For example, my recent work – SunSpot has demonstrated that solar generation data at a particular site embeds the location of that site, and this location information can be extracted from the solar generation trace using advanced data analytics and machine learning techniques. Then, I will discuss a low-cost obfuscation defense-Combine Heat and Privacy (CHPr) that I designed to preserve energy data privacy. CHPr can schedule large elastic heating loads already present in many homes (e.g., water heater) to reshape demand to protect occupancy effectively. Finally, I will discuss my future directions about cybersecurity and privacy research in energy systems and other intersect areas of CPS.

Bio: Dong Chen is a Ph.D. Candidate in the Department of Electrical and Computer Engineering at the University of Massachusetts Amherst. His research focuses broadly on big data analytics, cybersecurity, and privacy in the context of cyber-physical systems, such as the electric grid. He received an M.S. and Ph.D. from Northeastern University (China) in 2010 and 2014, respectively, and a B.S. in Computer Science from Xi'an Communications Institute in 2006. His recent research focuses on both developing a wide range of energy data analytics for smart meter and renewable energy data and designing techniques for strengthening the security and data privacy of cyber-physical systems. He has published over 20 research papers in these and related areas over the past decade. In addition, his work on energy analytics has been applied to real-world energy data, which he has made publicly available. For example, his recent work on Non-Intrusive Occupancy Monitoring and the associated data has been cited over 70 times.

Date: March 5, 2018

Time: 10:00 am

209 Computer Science Building

MISSOURI S&T