Computer Science Chair Candidate Seminar

Cyber-Physical Security Through Information Flow

Dr. Bruce McMillin, Missouri S&T

A Cyber-Physical System (CPS) is an engineered physical system with a significant cyber component and consists of many interacting distributed cyber and physical components. CPSs are deployed in critical applications such as such as advanced power electronics in a green electric power system, vehicles in an automated highway system, distributed aircraft navigation systems, chemical process plants, and consumer components of a smart house in which correct operation is paramount. Unintended or misunderstood interactions among the components of a CPS cause unpredictable behavior leading to serious errors. While each component may independently function correctly, their composition may yield incorrectness due to Interference. Interference that violates correctness or security is well-understood in the purely software (cyber) domain. In the CPS domain, interference is much less understood. Security and confidentiality problems are particularly vexing. Attacks such as Stuxnet show how formal security properties can be violated through physical interference with the cyber components. To add to the difficulty, CPS security is difficult to specify in terms of traditional "high" and "low" security.

This talk presents an interpretation of formal information flow properties and interference within the context of a cyber-physical system blending both physical and cyber information flow properties across multiple security domains. This poses the deep scientific question: how to make such systems secure and correct?

Bio: Dr. Bruce McMillin is currently a Professor of Computer Science, Associate Dean of Engineering and Computing, director of the Center for Information Assurance, co-director of the Center for Smart Living and a senior research investigator in the Intelligent Systems Center all at the Missouri University of Science and Technology. He leads and participates in interdisciplinary teams in formal methods for fault tolerance and security in distributed embedded systems with an eye towards critical infrastructure protection. His current work focuses on protection for advanced power grid control. His research has been supported by the United States NSF, AFOSR, DOE, NIST and several Missouri Industries. Dr. McMillin has authored over 100 refereed papers in international conferences and journals. He is leading the distributed grid intelligence project of the Future Renewables NSF Engineering Research Center, an advanced smart grid architecture. He is a senior member of the IEEE and member of the IFIP WG 11.0 on Critical Infrastructure Protection, and member and contributor to the SGIP Smart Grid Interoperability Panel. He currently serves in the IEEE Computer Society's Board of Governors and is a member of the Computing ABET Accreditation Commission.

Date: April 4, 2017

Time: 11:00 am Refreshments

11:15 am Talk

245 McNutt

MISSOURI S&T