Common Correctness for Protecting Confidentiality of Critical Infrastructure Systems

Investigators:
Bruce McMillin, Sahra Sedigh, Daniel Tauritz, Ann Miller

Funding Source:
Department of Defense

Project Description:
Certain potential risks of large-scale critical networked systems have gained widespread recognition, e.g., cascading failures of power systems. Further, the number, speed, and sophistication of attacks on networked systems are increasing dramatically. There is a clear need for improved methods of information and system assurance. Essentially all critical infrastructures are cyber-physical systems which have a physical/real-time component that manages aspects such as power flow, water pressure, and gas temperature. Our view is that it is impossible to assess the “correctness” of a system without enmeshing the physical and cyber aspects, e.g., physical models and the data representing them. The goals of this proposal are to develop a system science and to build a workforce for Critical Infrastructure Protection that is capable of assessing these combined entities. Unfortunately, there is a large impediment to this effort, namely that domain experts and IA professionals speak different “technical languages”. The work described in this proposal offers IA professionals a chance to break that barrier. A cooperative relationship with the University of Arkansas at Pine Bluff seeks to expand the pipeline of students entering the computer security field.

Publications:


