Multi-dimensional Security in Energy Cyber-Physical Systems

A position paper for the 2013 National Workshop on Energy Cyber-Physical Systems

Joseph J. Januszewski, III, CISSP

Security in the energy sector can be envisioned as a multi-dimensional game of chess, with multiple players representing various actors, presenting threats of differing levels of complexity. Each tier creates an abstraction thereof, comprised of a multitude of discrete components representing various assets and, by extension, threats. By elucidating each tier, while providing a detailed schema for protection, defense and attack vectors, the larger infrastructure can be represented, and a mechanism of defense in depth can be implemented to repel those vectors.

By examining the electrical infrastructure, and creating various layers of resources, including applications, communications, controls, facilities and corresponding physical devices, themselves, we can develop a mechanism design extracted from game theory to analyze the multiplicity of threats to assets at each tier, then extrapolate the combinations of threats that would exist across the various layers.

A basic example is the automated metering infrastructure (AMI). The AMI consists of several applications, a communications mechanism, various controls and facilities (such as the meter itself located at a customer's premises, as well as the back-end systems for consumption throttling, tracking and billing processes), while also representing a physical device presenting an attack surface of the internal network. The AMI represents only one aspect of the cyber-physical realm to examine in securing the electric infrastructure.

This proposed presentation will address the infrastructure in multiple verticals, including distribution, transmission and generation, illustrating how they form one axis of the attack surface, while providing multiple layers and tiers all their own. The Critical Infrastructure Protection (CIP) protocol, developed by the North American Electric Reliability Corporation (NERC), can be aligned with these security risk assessment paradigms, further providing a more cohesive set of policies through threat and attack vector analysis.

The author, Joseph J. Januszewski, III, is a practitioner in information and operational security. He has worked in information technology, information security and electrical engineering in both the public and private sectors for over 25 years. For the past five years, he has been involved with the design and security of industrial control systems, with a focus on Smart Grid technologies. A member of various groups, including the DHS Industrial Control Systems Joint Working Group (ICSJWG), the Critical Infrastructure Partnership Advisory Council (CIPAC), the IEEE Power Engineering Society Smart Grid Roadmap Task Force, the ISA99 Committee on Industrial Automation and Control Systems Security and the NBISE Smart Grid Cyber Security Panel. A senior member of the IEEE and Fellow of the NBISE, Januszewski also serves as a subject matter expert for the National Institute of Standards and Technology, the Department of Energy and the Department of Homeland Security.