A Multi-Layer Defense for Power Grid SCADA Systems

Joseph Giampapa

Power grid SCADA (supervisory control and data acquisition) systems provide remote sensing and control for the remote and distributed power grid functions of: generation, transmission and distribution. Traditionally, a power system SCADA system has been maintained as a separate system that has been isolated from the rest of the information technology (IT) components of power system control centers. But as business pressures mount within the power industry to provide more time-sensitive, highly responsive and cost-effective means of generating and delivering electricity, those barriers are eroding and there has been increased awareness of the possible vulnerabilities of SCADA systems to cyber-attacks. One of the most dangerous and easily executable cyber-attacks is called a false data injection (FDI) attack, whereby the data provided by the SCADA system to state estimation is modified in such a way that the power grid operator observes the operating state of the grid to be other than what it actually is. Making decisions with incorrect perceived state can lead to unsafe operating conditions, damage expensive and hard-to-replace components, lead to power failure, or even lead to loss of human life.

Investigations into the effects of FDI cyber-attacks have been published in the power systems, control theory, and IT communities, focusing on three research areas, in general: vulnerability analysis of state estimation, consequence analysis on the multiple energy management system functions that rely on state estimation, and the development of countermeasures. The solutions, however, are typically proposed from community-centric perspectives. For example, IT researchers propose intrusion detection schemes, data and command encryption, firewalling, best coding practices, and a variety of security measures that represent current best practices in the IT industry, but cannot address what to do if, notwithstanding the best IT security measures, the SCADA system has been compromised. Control theorists and power systems analysts approach the problem from an architectural perspective: how many measurement devices need to be compromised, how should measurement values be modified to initiate an attack, and what should be the degree of heterogeneity of device types to reduce the likelihood of compromise? But such analyses do not consider what type of information needs to be accessed (e.g. the vector of attack) in order to plan and execute an attack, what information can be cross-referenced to confirm or refute the validity of data, and that changes in power grid state will produce changes in information state elsewhere in the control and management of a power grid.

My work in progress is to approach the defense of power grid SCADA systems as a problem of identifying and leveraging information that is present in the multiple layers of abstraction that are embodied in the design, operations, and business processes that revolve around power grid energy management systems. Some of those layers of abstraction are transversal to power grid operations: the physics or physical-electrical properties of the grid, the control theory model of the grid, the IT model of the grid, and the business model of the grid. Other layers follow the functional divisions of the energy management system architecture, such as: state estimation, automatic generation control, load forecasting, economic dispatch, and others. Information of relevance to validating SCADA data, and models for how to perform the validation, are encoded in autonomous software agents that, through local knowledge of grid architecture and their validation models, can provide verification of the SCADA data as it is fed into the centralized state estimator. Via ad hoc but model-drive communications, the autonomous agents can detect and isolate FDI cyber-attacks on power grid SCADA systems.