Cybersecurity Risks of Dynamic; Two-way Distributed Electricity Markets

Funded by:
NSF Grant: SES-161880

Principle Investigators (PIs):

Jason Dedrick,
jdedrick@syr.edu
School of Information Studies (iSchool), Syracuse University

Peter Wilcoxen,
wilcoxen@maxwell.syr.edu
Maxwell School, Syracuse University

Steve Chapin,
chapin@syr.edu
College of Engineering & Computer Science, Syracuse University

Overview

The U.S. electric grid is being transformed from a one-way channel delivering electricity from central power plants to customers at set prices, toward a distributed grid with two-way flows of information and electricity and dynamic pricing. The benefits of creating distributed markets for electricity are potentially great. Consumers can better manage their energy use, costly peak electricity load can be reduced through demand response, and dynamic markets can reward innovation by existing or new firms.

However along with these potential benefits come significant cybersecurity and privacy risks. Participants in distribution-level markets may be technically unsophisticated and use evolving energy management and communications systems that do not provide high levels of security. The potential cost of a security breach that overloads or shuts down large areas of critical infrastructure is immense.

The objectives of this research are to advance knowledge of cybersecurity risks in dynamic distributed markets for electricity, and to provide insights for policymakers, regulators and businesses by answering the following questions: (1) What are the potential security and privacy risks associated with various distributed electricity market designs and rules? (2) What security measures would be required to provide an acceptable level of risk under different market designs and rules? (3) What are the trade-offs between taking measures to reduce risks and optimizing market performance?

The research employs an innovative mix of research methods, including interviews, modeling of market structures, simulations using real world electricity use data, modeling of data flows, and security threat analysis. A discrete event simulation framework is used to model interacting agents that comprise distributed electricity markets and estimate a cost function for the relative welfare cost of a given grid topology and market policies. A software simulator is constructed and tested using real electricity use data to vary parameters on multiple dimensions and minimize cost. Security attacks are introduced into the simulations to identify impacts on grid stability, market trust and privacy.

Intellectual Merit

The research applies a multidisciplinary approach, including economics, computer science and public policy, to advance understanding of how the adoption of distribution-level electricity markets can introduce security and privacy vulnerabilities. A cost function model is estimated to compute the relative welfare cost of a market with given grid topologies and market policies. The use of real world data enables simulation of a wide array of different market structures and interactions with many bidding and response policies on the part of distributed consumers/producers and market controllers. The research is new and transformative in its development and use of modeling and simulation tools, tested with real data, to identify security and privacy risks associated with different market structures, security methods, and threat types.

Broader Impacts

The results of this research will be valuable in supporting decision making by policymakers, regulators, utilities and other market participants, and the cybersecurity community. They will be used to guide decision makers in designing market structures, mechanisms and rules for distributed electricity markets that balance economic benefits with security and privacy risks. Markets can be designed with safeguards to protect participants, ensure effective market functioning, and protect the electrical grid infrastructure.