Improving Security in the Growing Smart Energy Corridor

Successes from the Long Island Power Authority Smart Grid Demonstration Program Project

Introduction

In New York, the [Smart Grid Demonstration Program] (SGDP) project of the Long Island Power Authority (LIPA) is improving cybersecurity while expanding the advanced metering infrastructure (AMI). Located on Long Island along New York business route 110, the *Smart Energy Corridor* demonstration project began in February 2010 and runs until February 2015. Partners include the Research Foundation of the State University of New York (SUNY) at Farmingdale and the Research Foundation of SUNY at Stony Brook.

LIPA, the country's second-largest utility in terms of revenue, operates from Long Island, NY, and serves 1.1 million customers. It is modernizing its electric distribution systems with a $25.3-million cooperative research agreement including $12.5 million of U.S. Department of Energy funding under its Smart Grid Demonstration Program. With this Recovery Act funding, LIPA is creating a smart energy corridor by demonstrating the integration of AMI technology with other technologies to serve various smart grid applications.

Already, LIPA has added 2,550 new smart meters and a customer web portal during the demonstration project. Other AMI additions include six pad mount housing (PMH) underground switches, 17 automatic sectionalizing units (ASUs), and 51 two-way capacitor bank controllers.

Fuzzers, Rapid Response Aid Cybersecurity

Smart meters use a "defense in depth" strategy to resist attacks. Their defenses include frequency hopping cryptography to resist eavesdropping and message tampering attacks, and careful coding to avoid well-known classes of vulnerabilities, such as buffer overflows. The LIPA cybersecurity team at SUNY at Stony Brook found that frequency hopping alone is not sufficient to resist eavesdropping and message injection attacks.

Figure 1. Smart Meter

They are further evaluating meter security using a type of computer software program known as a fuzzer. This software detects security bugs by sending invalid messages to specified target devices. If the target devices do not respond appropriately to the invalid messages, it indicates that a bug is likely.

“The security team has not found any serious security flaws in the meters we’ve deployed on our network,” said Ming Mui, principal investigator for the LIPA demonstration project. “We will continue to evaluate meter security, but the results have increased our confidence in the security of our network.”

“This blue-sky research shows how to build cybersecurity systems that can react to new attacks and vulnerabilities that are discovered after deployment.”

In another area, the research team demonstrated how a specialized compiler that analyzes computer code can work with a network-alert system to protect virtually all nodes against attack. The system enables a node that detects an attack to alert other nodes in the system and provide them with the information they need to protect themselves from the cyber-attack. The nodes can quickly spread this defensive knowledge throughout the network, effectively containing the attack.

“This blue-sky research shows how to build cybersecurity systems that can react to new attacks and vulnerabilities that are discovered after deployment,” Mui said. “This capability is crucial for critical infrastructure that must operate continuously for years, if not decades.”

Customers Involved in Monitoring Energy Use

With improved cybersecurity comes the opportunity for greater customer involvement, a desired result of the smart grid. To help customers learn about more efficient energy use, researchers developed and provided a web portal tool for customers who received an AMI meter. So far, the portal has proven useful. Customers report that the usage and cost data provided by the portal helps them reduce their energy use and costs.

“Having customers better understand their energy use is the first step towards consumption-behavior change,” Mui said.

Figure 2. Cyber Security Test Bench

Hurricane Sandy's Lessons Continue

In late 2012, the course of the LIPA demonstration project drastically changed when Hurricane Sandy hit the eastern U.S. In spite of the devastation, LIPA took advantage of the opportunity to learn about adapting the smart grid to function in inclement weather.

"Sandy accentuated the importance of training to complement automation."

Not surprisingly, researchers found that during fair weather and moderate storms, distribution automation (including ASUs and PMHs) continued system operations by performing circuit switching to minimize the number of customer outages.

In areas of greater devastation, however, due to Sandy's prolonged power outages, the energy stored in the batteries that operate the ASUs was depleted, necessitating manual operation of distribution switches.

According to Mui, "Sandy accentuated the importance of training to complement automation."

Next Steps

In Hurricane Sandy's aftermath, LIPA is working with suppliers on extended-life batteries and will be providing additional training to restoration personnel.

To increase public understanding about the safety of AMI technologies, LIPA researchers are now working with SUNY at Stony Brook to perform electromagnetic field testing of AMI meters. The AMI meters' electromagnetic fields will then be compared to those of common household appliances.

Further Reading

For more information about the LIPA demonstration project, read its Interim Technology Performance Report, published on the SmartGrid.gov website. A more detailed description of SGDP can also be found at SmartGrid.gov.

Under the American Recovery and Reinvestment Act of 2009, the U.S. Department of Energy and the electricity industry have jointly invested over $1.5 billion in 32 cost-shared Smart Grid Demonstration Program projects to modernize the electric grid, strengthen cybersecurity, demonstrate energy storage, improve interoperability, and collect an unprecedented level of data on smart transmission, distribution operations, and customer behavior.