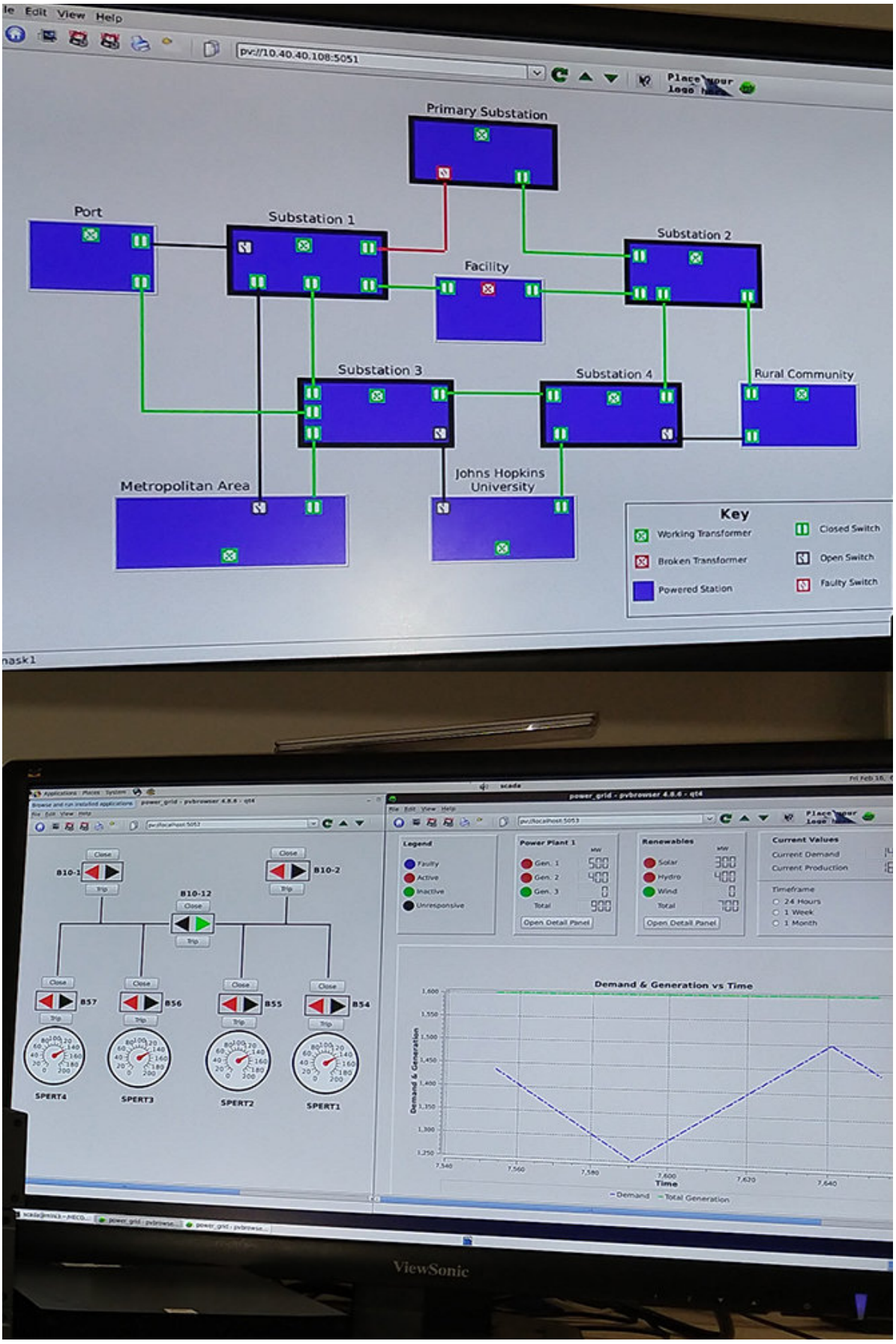
Hacker-resistant power plant software gets a glowing tryout in Hawaii

February 26 2018, by Phil Sneiderman


Edit View Help
pv://10.40.40.108:5051
Primary Substation
Port
Substation 1
Substation 2
Facility
Substation 3
Substation 4
Rural Community
Metropolitan Area
Johns Hopkins University
Key
Working Transformer
Broken Transformer
Powered Station
Closed Switch
Open Switch
Faulty Switch
B10-1
B10-2
B10-12
B57
B56
B55
B54
SPERT4
SPERT3
SPERT2
SPERT1
Legend
Power Plant 1
Renewables
Current Values
Demand & Generation vs Time
Demand & Generation
Time
Demand
Total Generation
ViewSonic

These screen images depict a Johns Hopkins cybersecurity team's open-source Spire software, which is designed to resist hacking attacks that seek to disrupt a power plant's control system. Credit: Johns Hopkins University

Johns Hopkins computer security experts recently traveled to Hawaii to see how well their hacker-resistant software would operate within a working but currently offline Honolulu power plant. The successful resilience testing, funded by the U.S. Department of Defense, was triggered in part by growing concerns about the vulnerability of electric power grids after two high-profile cyber-attacks turned out the lights in parts of Ukraine during the past two years.

Neither outage in Kiev was long or extensive enough to cause serious harm or panic. Yet the attacks served as a wake-up call, putting a spotlight on power grid security in the United States and elsewhere.

"Today, our power system is not designed to withstand the kind of attacks that happened in Ukraine," said Yair Amir, professor and chair of the Department of Computer Science in the university's Whiting School of Engineering. "If even part of a power grid's control system is compromised, the game is over. We need to make our grid more secure, resilient and intrusion-tolerant."

Amir and his team of researchers hope to help boost resilience with their new open-source control system for power grids called Spire. The intrusion-tolerant system is designed to keep power flowing even if part of the system is compromised.

In an experiment last April, a Sandia National Laboratories hacker team

was able to remotely obliterate a commercial grid control system within a couple of hours, but the team could not penetrate the Spire system for three days. On the third day, the Sandia attack team was given remote access to part of Spire, but its test hackers still could not disrupt the system's correct operation.

More recently, the Spire developers from Johns Hopkins were invited to get their feet wet in Hawaii. At the end of January, Amir and his team went to an offline Hawaiian Electric Company plant in Honolulu and spent two weeks testing the Spire system on the power plant's equipment with the help of HECO engineers Keith Webster and John Tica. After a few days of setup and integration, Spire ran continuously without interruption for almost a full week.

The goal of the Hawaii deployment was to verify that Spire can operate without degrading the control system's performance and without adverse effects on other power plant systems.

A power grid needs to respond to adverse events—say, a circuit breaker tripping or a generator shutting down—within hundreds of milliseconds, Amir said. "If a generator goes out, the system needs to quickly detect it and compensate by increasing power in other generators or by cutting power to parts of the grid."

On the last day of the Hawaii test, Webster deployed a device to measure end-to-end reaction time of the commercial control system in the plant and of Spire. The measurements showed that the commercial system reflected a change in the grid's power state within 900 milliseconds to one second. Spire showed the same change within 400–500 milliseconds, meeting the timeliness requirement.

Part of how the system works is with the help of replicas. The researchers built it to contain six copies of the main control server that

work together to agree on updates in the system. That's the smallest number of replicas needed to get good protection, Amir says. "Each replica votes on every data and decision," he added. "If one of the replicas is compromised and another is going through maintenance, then the other good replicas will enable the system to continue working properly and in a timely manner."

Why was the test conducted in Hawaii? First, the research project was funded by the Department of Defense, which is one of HECO's largest customers. In addition, Amir said, the unique access to a "mothballed" power plant with fully functional control systems but without active power generation was perfect for grid-level control system tests. "If something goes slightly wrong," he said, "at least you don't have a quarter million people losing power."

Amir and his colleagues plan to release Spire 1.1, the version that was deployed in this test-deployment, in the coming weeks. Version 1.0, tested in April, is already available for download.

Making Spire open-source was kind of a "no-brainer," Amir said. He has spent over a decade of his research career working on intrusion-tolerant systems and networks. He said that releasing the source code openly increases awareness and the chance for real-life impact. The U.S. power grid is a logical target for major cyberattacks, he said. Disabling or tampering with the grid on a large scale, Amir said, could seriously harm the country by disrupting lives and causing immense economic loss.

"We decided that we won't just publish our results," he added, "but we will release open-source solutions that will show people how to make control systems for the power grid secure, resilient, and intrusion-tolerant," Amir said. "We want to create a community of people who are really interested in that. We need to protect our critical infrastructure."

Provided by Johns Hopkins University

Citation: Hacker-resistant power plant software gets a glowing tryout in Hawaii (2018, February 26) retrieved 23 April 2024 from https://techxplore.com/news/2018-02-hacker-resistant-power-software-tryout-hawaii.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.