Quarterly Update

Pacific Northwest SMART GRID DEMONSTRATION PROJECT

Summer 2012

Cybersecurity and the PNW-SGDP

"Protecting the castle" in terms of providing a reliable, secure electricity system is a top priority for the Pacific Northwest Smart Grid Demonstration Project. Keeping the electronic bad guys at bay is something most people don't think about every hour, every day, but at the project, we can't afford that luxury.

If you haven't experienced a virus on your computer, you've undoubtedly read about one in the news. And like a sickness, computer viruses often are spread easily by social interaction such as sharing flash drives – a seemingly benign exchange. Viruses, worms, malware, spyware and other grim-sounding computer ailments can be simply annoying – slowing down your computer. Or a virus can be devastating – causing infrastructure collapse. And although many viruses are spread through sophisticated programs, it's quite alarming how a simple act of opening an attachment, even from a trusted source, can cause so much damage, so quickly.

With the evolution of Smart Grid, where two-way communication at every point in the electrical system from generation to end-users is the long-term goal, cybersecurity is profoundly critical. This edition of our quarterly newsletter will take a look at cyber security in general, and focus in on the Pacific Northwest Smart Grid Demonstration Project's stringent cyber security program.

Ron

Ronald B. Melton, PhD
Project Director

What's inside

Project Objectives and Attributes

Primary Objectives:

- Develop and validate an interoperable distributed communication and control infrastructure using transactive control signals;
- Measure and validate smart grid costs and benefits;
- Contribute to the development of standards and transactive control; and
- Apply smart grid capabilities to support the integration of renewable resources.

Operational Objectives:

- Manage peak demand;
- Facilitate wind integration;
- Address constrained resources;
- Improve system reliability;
- Improve system efficiency; and
- Select economical resources.

Key Attributes:

- Leave an installed operational base of smart grid assets and successful operational strategies for the region.
- Stimulate the regional and national economy by creating jobs and a vibrant smart grid industry.

Destruction at the speed of light

According to best-selling Richard A. Clarke's book *Cyber War,* "If they take over a network, cyber warriors could steal all of its information or send out instructions that move money, spill oil, vent gas, blow up generators, derail trains, crash airplanes, send a platoon into an ambush, or cause a missile to detonate in the wrong place." Clarke says that electric utilities are right up there with our nation's defense and financial systems in terms of needing protection in the form of cyber security.

Stuxnet is an example of malware directly targeting a specific energy facility. Stuxnet attacked supervisory control and data acquisition systems, otherwise know as SCADA, of a specific nuclear facility in Iran. Utilities regularly use these systems to help keep the lights on. Stuxnet demonstrated that malware could be used to attack energy control systems.

Bora Akyol, Ph.D., PNW-SGDP Cyber Security Lead, describes the cybersecurity program for the Pacific Northwest Smart Grid Demonstration Project, which is testing a unique communication protocol. "We use an iterative approach, which means that we are constantly monitoring, learning and updating our cybersecurity efforts," Akyol says, and adds that this approach follows industry standards and guidelines established by the National Institute of Standards and Technology. "We constantly add new tools and build on the information we learn. The goal is to automate the system as much as possible to reflect the growing body of knowledge."

Akyol says inter-organizational coordination is the biggest challenge in the PNW-SGDP cyber security planning and implementation.

"We must work with 11 external utilities and several other organizations. We've established boundaries that we control – we strictly limit what goes in and what goes out. If a utility or other partner were to have an incident, we try to minimize the chance of the problem jumping from one participant to another."

The PNW-SGDP used a risk-based approach in establishing its cybersecurity plan. "We didn't just install off-the-shelf firewalls and protocols," Akyol says. "We started from scratch. We looked at topology, connectivity, and many other factors, and then we developed 40 pages of risks. We prioritized the risks, developed mitigation techniques, and identified the remaining residual risk. It was a very thorough, exhaustive process."

The project also uses the commercially available "Splunk" – a cyber security event data monitoring and alerting product. Splunk collects and indexes data in real-time, and it generates alerts and reports.

As malware, viruses, spyware and other menaces to critical infrastructure evolve and mutate, the PNW-SGDP's cyber security experts, and the programs they develop and implement, will do their best to stay ahead of the threat. It's a never-ending game. Bora Akyol says that facet of the job is what keeps every good cyber security practitioner awake at night.

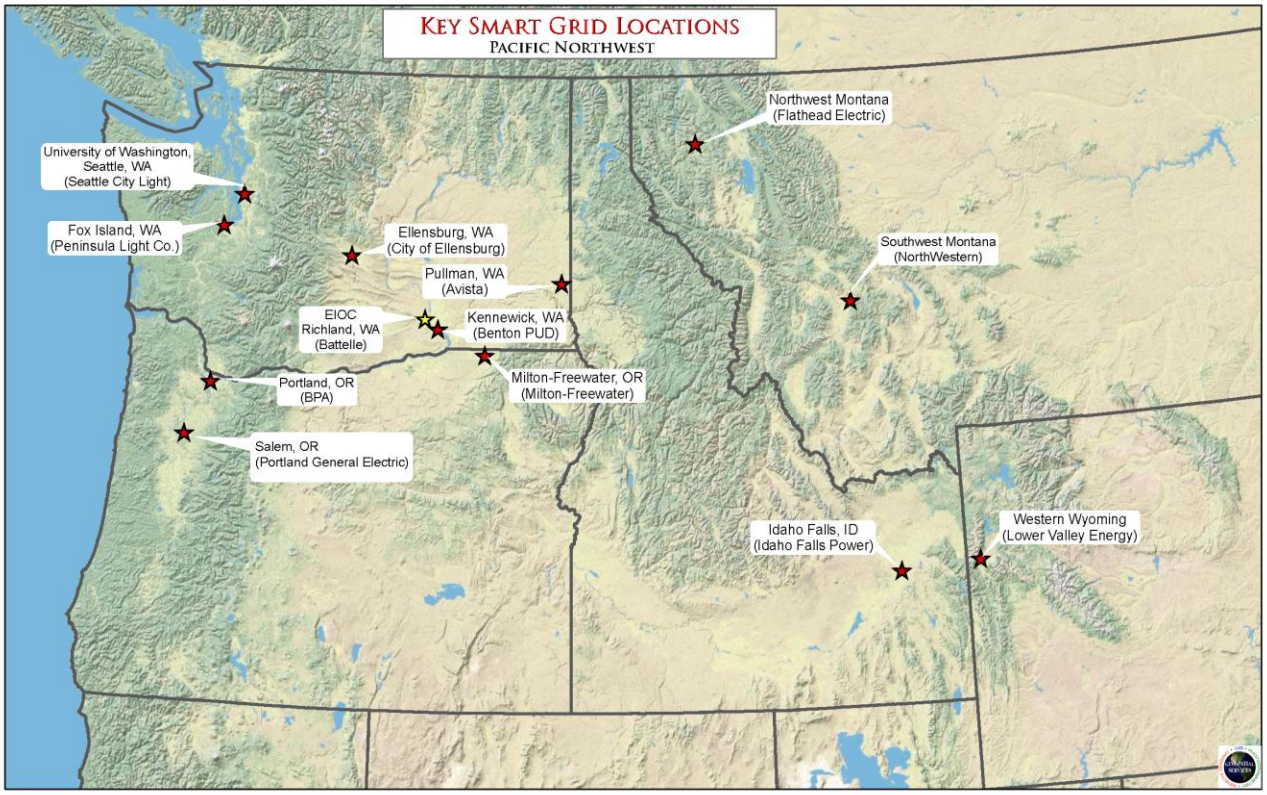
As ARS Technica reported this June, "Stuxnet is old news by now. Even the newly discovered "Flame" malware was developed some time ago. While details about these two targeted attack packages are finally emerging, the next generation of attack tools has no doubt been developed and likely deployed."

At the end of the day, effective protection against cyber threats comes down to people being vigilant and following security protocols. Glad we have Bora and his team addressing the Pacific Northwest Smart Grid Demonstration Project's cyber security efforts.

Outreach calendar:

- June 7 – Avista held its first recruitment focus group for the smart thermostat pilot program.
- June 18 – Idaho Falls Power, during an "Electric Vehicle Day" celebration, presented four new Chevy Volts which will be part of the PNW-SGDP. They will test the interaction of the transactive control signal with the cars' charging. (See photo)
- June 26 – BPA presented at the National Town Hall Meeting on Smart Grid and Demand Response in Washington, D.C.
- Sept 5 – IBM Smarter Analytics live webinar with Ron Melton.
- Sept 25 – Presentation on the Pacific Northwest Smart Grid Demonstration in Nice, France in conjunction with the next ISGAN Executive Committee meeting.
- Sept./Oct. timeframe: Kick-off for transactive control signal go-live.

Dennis Stiles, Battelle's Energy Manger attends the Idaho Falls Power event to inaugurate four new PHEVs that will interact with the Transactive Control Signal.



Project description

The Pacific Northwest Smart Grid Demonstration project is a regional endeavor funded by the Department of Energy under the American Recovery and Reinvestment Act of 2009. The goal is to verify the viability of smart grid technology and quantify smart grid costs and benefits. This information will help validate new smart grid business models at a scale that can be adapted and replicated nationally.

With the 50 percent DOE matching funds, this project has a $178 million budget.

Smart grid can help meet increasing power demands, reduce greenhouse gas emissions, promote energy independence, enhance reliability and help improve national security. It is a system that uses technology to enhance power delivery and use through intelligent two-way communication. Power generators, suppliers and users are all part of the equation.

With increased communication and information, smart grid can monitor activities in real time, exchange data about supply and demand and adjust power use to changing load requirements. Smart grid technology includes everything from interactive appliances in homes to substation automation and sensors on transmission lines.

The regional project, the largest smart grid demonstration project in the nation, is led by Battelle Memorial Institute, Pacific Northwest Division. Participants include the Bonneville Power Administration, utilities, universities and infrastructure partners. It includes 112 megawatts of responsive resources and will last for five years.