Innovation

Securing the Grid's Edge

EPRI to Develop Secure 'Architectures' for Distributed Energy Resources

By Scott Sowers

If a private firm installs an Internet-enabled solar array on a homeowner's roof and it gets hacked, who would be responsible for addressing the breach? Could the hackers impact grid operations?

"Today, various companies install large numbers of solar arrays, lease them back to the property owners, and manage them through Internet-based communications," said Galen Rasche, EPRI senior program manager for cyber security. "If any of these companies have security problems, they can impact distribution grid operations."

For an integrated grid, this emerging cyber security concern emphasizes the importance of securing distributed energy resources (DER) and consumer equipment, including rooftop solar.

"Security is important throughout the grid, but with DER, it can be easily overlooked because there are many parties involved—utilities, customers, makers of home energy management devices, solar installers, and companies that use cloud-based software to monitor grid-edge devices, such as rooftop solar arrays," said EPRI Senior Technical Leader Candace Suh-Lee. "This introduces more risk."

Developing Secure Architectures, Informing Stakeholders

EPRI is launching a project in 2017 to examine cyber security for grid integration of DER and to develop more secure communications architectures for protecting the grid and customer privacy.

EPRI will identify DER-related security objectives, risks, and possible roles and responsibilities of the various parties involved. Preliminary findings reveal uncertainty both in determining responsibility and in the lack of common architecture guidelines and roadmaps.

> "The results of this research will help regulators, the public, and other stakeholders better understand the challenges and determine the appropriate mix of standards, technology, and policy to address them."

"Today we have a multi-party grid," said Rasche. "Utilities can't be the only parties responsible for security because they're not able to monitor and control everything. All the parties have to do their part."

In EPRI's Knoxville laboratory, researchers will bench-test DER system components with security assessment tools, such as vulnerability scanners, protocol analyzers, and penetration testing software.

They will evaluate how devices react to common attacks, such as "replay attacks," in which a hacker captures a legitimate message and sends it to a device in different time and context. Another common hacking technique is called "fuzzing."

"Hackers try to 'fuzz' a device when they send malformed messages to it to see how it reacts," said Rasche.

Researchers will assess utilities' DER architectures, devices, and components and evaluate their security solutions.

“We’ll check systems and devices in the field for vulnerabilities and assess DER communications to see if they are properly protected, or assess the extent to which someone could compromise the security of the data,” said Suh-Lee.

EPRI is researching ways to help utilities monitor the cyber security status of grid-edge devices and networks.

“Utilities will want to monitor data traffic on the grid’s communications infrastructure to determine whether systems are behaving as expected,” said Rasche. “They may find that some data was supposed to be protected, but was not. Or they may find that some traffic patterns are not normal—a sign that something might be configured incorrectly or that a cyber attack may have occurred.”

“If security gaps can be addressed with existing technologies, we will include those in the architectures we are developing,” said Suh-Lee. “If not, identifying the gaps will help us to direct future research or to make recommendations to standards bodies.”

“The results of this research will help regulators, the public, and other stakeholders better understand the challenges and determine the appropriate mix of standards, technology, and policy to address them,” said Suh-Lee.

Key EPRI Technical Experts

Candace Suh-Lee, Galen Rasche