Protect, Detect, Respond, Recover

EPRI Project to Develop Comprehensive Cyber Security Guidelines for Power Plants

By Scott Sowers

Two days before Christmas in 2015, a coordinated series of cyber attacks knocked parts of Ukraine's electric grid offline, and nearly a quarter of a million residences lost their lights and heat for several hours.

The attacks, directed at three regional electric distribution companies, demonstrated prowess in several complex hacking techniques. These included spear phishing to obtain faked credentials, exploiting vulnerabilities in Microsoft® Office® documents, and deploying Black Energy 3 malware to infiltrate the utilities' networks and connected infrastructure such as uninterruptible power supplies.

The perpetrators were able to obtain login credentials to the utilities' virtual private networks, allowing access via the Internet to manipulate supervisory control and data acquisition (SCADA) servers. With this, they moved to cut off power to substations and change passwords. Locked out of their computers, utility staff watched the substations go offline one by one. The attackers then bombarded the distribution companies' call centers with thousands of calls, denying access to customers reporting outages.

Investigations revealed that the attacks were enabled by months of reconnaissance to learn the various systems, find weaknesses, and devise strategies to impact components.

"Once again, this past December there was another cyber attack on the Ukrainian grid, making it two attacks in a year. The repeated nature of these incidents reflects how electric power infrastructure is a potential target," said EPRI Senior Technical Leader Justin Thibault. "Generation control systems are moving into a new digital era with more automation. They are becoming more connected—potentially decreasing the cost of ownership, but increasing vulnerability to attacks."

EPRI has launched comprehensive R&D to develop cyber security guidelines and technologies for bulk power generation. This builds on four years of collaborative research in EPRI's Generation Sector on electric system security.

"In 2012, EPRI and a small group of utility members started a project looking at cyber security for instrumentation and controls in bulk power generation facilities," said Thibault. "In subsequent years, it grew to more than 20 members and produced six reports on topics such as security status monitoring."

A key insight from this work: Cyber security for generation can draw on lessons learned from security efforts in utility information technology (IT) departments. Power plants employ operational technology (OT), which uses computer hardware and software to control switches, valves, pumps, and other devices.

"The IT world has been dealing with cyber security for decades," said EPRI Principal Technical Executive Annabelle Lee. "We need to take the techniques that have worked for IT and apply them to the OT side."

The North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection Standards now require more sophisticated security strategies for a growing number of components and systems. While the proliferation of digital components makes the electric power system more interconnected and potentially vulnerable, the upside is that many new devices have built-in cyber security.

Power plants have several attributes that can support cyber security. Plant systems are usually contained within discrete security perimeters, with assets close to control room personnel who can physically disconnect devices from networks. Plants have significant instrumentation for monitoring and controlling various systems, making it easier to detect unusual network behavior.

EPRI's initiative aims to develop a spectrum of security strategies that protect plant computer networks with multiple mechanisms, so that if one fails, another is ready to stop an attack. Research focuses in three areas: Protect, Detect, and Respond and Recover.

Protect

To secure critical components, most power generation plants use *network segregation*. This involves separating external connections to control systems with unidirectional gateways or limiting physical connections to outside networks (also known as *air-gapping*). However, recent control systems intrusions demonstrate that disconnection from the outside is not sufficient protection against a cyber attack.

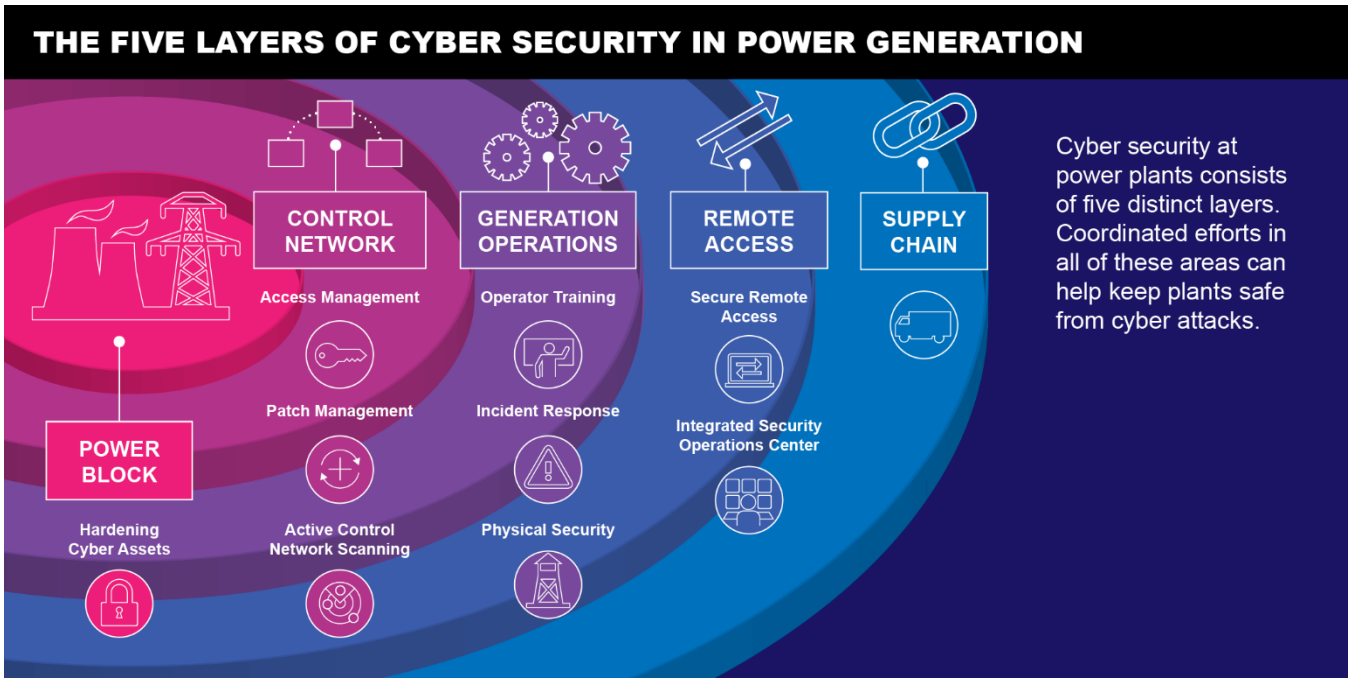
"Depending on network segregation alone to secure a control network would be like a bank with only one form of protection—doors that lock," said Thibault. "Most air-gapped systems can be compromised by personnel using thumb drives or other external media (as with Stuxnet) and by temporary network connections granted to external parties."

The computer "worm" Stuxnet was spread through thumb drives and targeted specific control components. It is believed to have damaged centrifuges at Iranian uranium enrichment facilities in 2009 and 2010.

EPRI is looking at technologies to secure "interactive remote access," which requires anyone attempting to access control systems from outside a utility to go through an intermediate server that authenticates identity. The server filters out suspicious actors.

Regularly installing cyber security patches (multiple code changes) in key computer systems is important for addressing vulnerabilities, and EPRI is examining their application in power generation. As the volume of malware has increased, so has the importance of performing the right system updates at the right time. Applying patches can be challenging because it often requires systems to be taken out of operation, potentially affecting power availability.

Devices can be “hardened” to reduce their “attack surface.” A valve actuator presents a relatively small attack surface, while a digital control system’s more complex attack surface likely requires additional layers of security. An example of hardening: Unnecessary software is removed and default passwords are changed to reduce the attack surface.



Detect

A big challenge with cyber security is that the victims rarely know that they are under attack until damage is already done. The staff at the Ukrainian distribution companies didn’t realize what was happening until they were locked out of their own accounts, watching outsiders control their systems. EPRI researchers are examining emerging detection technologies that can alert utility personnel to potential threats and attacks.

“Most cyber security breaches go undetected for months and sometimes years,” said Thibault. “Breaches are most often discovered when law enforcement contacts the victims or when the consequences of the breach have become apparent.”

Detecting an attack requires an ability to identify anomalies in networks and systems. This involves training personnel to recognize attack signs and deploying technologies such as intrusion detection systems, intrusion prevention systems, and security information and event management systems.

“We are seeing more cyber security companies develop intrusion detection systems for industrial control systems and networks,” said EPRI Senior Program Manager Galen Rasche. “Rather than relying solely on the traditional signature-based approach, these products also establish baseline system readings for a network’s behavior and look for unusual behavior.”

Detection must be accurate to be effective, and threat management can help. These techniques are used to collect and interpret information about security threats from reliable sources and characterize intent, capability, and targets.

Rasche points out that security companies are improving the exchange of threat information among computers and systems to facilitate detection and a speedy response. “The goal is to quickly share key indicators of compromise for specific cyber threats, enabling security staff to proactively detect and thwart a threat before it turns into a larger incident,” said Rasche.

Respond and Recover

Ukraine’s 2015 outage was corrected within hours, but repairing system damage took months. A speedy recovery is critically important because the primary objective of power generation is availability.

“After securing a system that has been breached, a utility must be able to restore the system fully and quickly,” said Thibault. “This is achieved with good planning—systems are backed up in advance, the configurations of various components and systems are well known, and processes are in place to restore them. Properly classifying cyber security incidents helps to determine the best course of recovery actions.”

After recovery, *forensic analysis* is used to identify, preserve, recover, analyze, and present facts about the attack, helping operators understand how their systems were breached and how they can be improved.

“Forensic analysis also adds to the lessons learned and industry operating experience,” said Thibault.

“Doing Common Things Uncommonly Well”

There’s more to cyber security than simply deploying advanced technologies for protection, detection, and recovery. “A lot of doing security work is doing common things uncommonly well,” said Thibault.

Two “common” areas—configuration management and procurement—are fundamental to protecting power generation assets. In 2014, EPRI published guidance on implementing configuration management for digital control systems. Many cyber attacks exploit factory default settings, and effective configuration management can help protect against such intrusions. Carefully managing the installation of new components and keeping patches up-to-date eliminates many vulnerabilities.

Even with configuration management, the digital components themselves could be a security threat, given their design and manufacture. A 2013 EPRI report provides strategies for addressing security concerns in procuring digital assets.

EPRI plans to publish guidelines on other aspects of generation cyber security, along with “reference architectures” or templates for securing control systems and integrating future technologies. Also in the works is an online exchange for EPRI utility members to share research insights and operational experience.

“Cyber security for power plants is a multi-layered challenge, but it is not insurmountable,” said Thibault. “Developing best practices and more robust security will make it more difficult to infiltrate generation assets. When a power company chooses to avoid the challenge of implementing effective cyber security, it is choosing to live in the dark.”

EPRI R&D on Transmission and Distribution Cyber Security

Safeguarding generation plants is a big part of cyber security in the utility industry. Equally important is securing transmission and distribution systems. As grid devices become more interconnected through telecommunications networks, cyber security measures must be implemented to support reliable power delivery.

EPRI's Cyber Security and Privacy Program develops security requirements and metrics, guidelines for risk assessment and monitoring, and tools and technologies to assess security and manage grid devices and threats. For example, researchers are:

- Incorporating security into various grid components and developing approaches for utilities to meet regulatory requirements
- Examining ways to gather near real-time knowledge on the system and security status of substations, field devices, and other parts of the grid
- Establishing plans and technologies to detect and respond to cyber attacks while maintaining power delivery
- Identifying threat hunting approaches, tools, and methodologies for operational technology

Key EPRI Technical Experts

Justin Thibault, Annabelle Lee, Galen Rasche, Matt Gibson, Mike Thow