In Development

A New Approach to Safeguard “Attack Surfaces”

EPRI Develops Classification Scheme to Help Protect Nuclear Plants from Cyber Attacks

By Margaret L. Ryan

A term of art in cybersecurity is “attack surface analysis,” and it’s a key to the process that EPRI is developing for nuclear plants to help identify and block entry points for cyber attacks before hackers can find them.

“Attack surface is a more precise way to talk about the types of holes or doors into your device,” said EPRI Senior Technical Leader Matt Gibson.

The U.S. Department of Homeland Security logged more than 256 industrial cyber security incidents in 2013, more than half of them in the energy sector. Targets included power plants and critical grid infrastructure. Power plants historically operated with isolated, proprietary control systems, but with the advent of regional power pools and smart grids, they’re increasingly connected to the outside world. Cyber attackers can potentially exploit hundreds of digital components. These range from simple switches and measuring devices to complex computerized systems that monitor and balance electricity flow to and from the plants. All of these create myriad electronic pathways that must be properly secured.

According to Gibson, nuclear power plants already have significant cyber security. The most sensitive control equipment, which monitors, manages, and protects plant process systems, is not connected to the Internet. However, the attack surface includes interfaces where patches and updates are added from portable storage media, and those surfaces must be digitally secured.

“While nuclear plant owners have committed significant resources to cyber security, the industry always takes a ‘belt and suspenders’ approach to safety,” said Gibson. “Nuclear operators wanted EPRI to provide a systematic way to verify that potential vulnerabilities are being identified. They want to confirm that they are at the level of technical detail needed to secure plant systems and allocate security budgets effectively.”

Organizing Attack Surfaces into Profiles

EPRI is developing and validating an integrated classification scheme that recognizes when attack surfaces of different plant equipment are the same. Based on the classification, researchers can identify measures to block each potential attack pathway, regardless of the specific device.

“A lot of different devices have the same cyber attack surface,” Gibson said. “We are trying to organize those attack surfaces into a set of characteristic profiles so utilities don’t have to analyze every single device. If your attack surface matches a profile that will give you things you can do to protect the device.”

To classify attack surfaces methodically, researchers began with small, single-function digital devices, which typically have fewer external interfaces. Devices such as valve actuators, valve positioners, and instrument transmitters do not have general purpose network connections or memory cards and other removable media. Researchers are finding that they have smaller attack surfaces.

Nevertheless, it is proving essential to analyze devices individually. “Devices with more complex functions do not necessarily have a larger attack surface,” said Gibson. “Complex controllers can have a small attack surface, while functionally simpler devices may have multiple points for potential intrusion. It is challenging analysis.”

Expanding the Analysis

EPRI will apply the analysis to progressively more complicated equipment, such as network interfaces and programmable devices, which tend to have larger attack surfaces as a consequence of multiple points of interface with other systems.

The attack surface approach is enabling EPRI to develop a methodology that can be applied consistently across devices, nuclear plants, and the industry. The project's first technical report was issued in 2015. EPRI will test the approach at operating nuclear plants in 2016.

Key EPRI Technical Experts

Matt Gibson