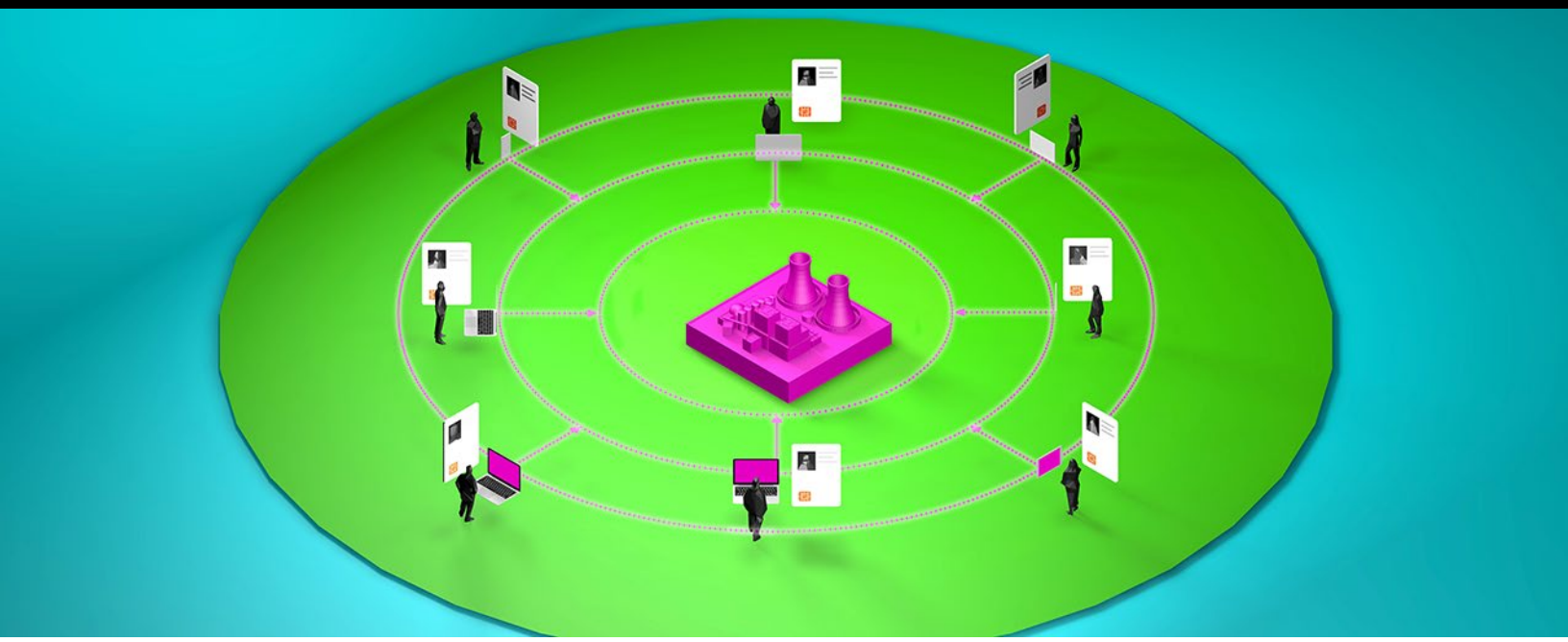


A New Tool to Protect the 'Keys to the Kingdom'

EPRI Develops System to Help Improve Remote Access Security for Power Plants

By Chris Warren

A cyber attack on an oil and gas facility last year was deemed by experts a "watershed" event that could usher in a new wave of similar attacks on industrial facilities.

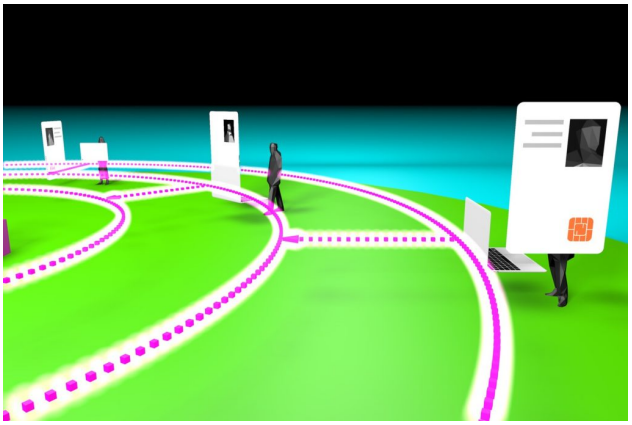
The attackers gained access to the plant's safety controls, manufactured by Schneider Electric and widely used in the energy industry. Malware deployed by the attackers caused the facility to shut down.

"While previous attacks on energy industry facilities focused on production systems, this was the first breach that targeted a plant's safety system," said EPRI Principal Project Manager Jason Hollern. "This indicates that adversaries have moved the needle on what they are willing to do."

"United States officials, their allies and cybersecurity researchers worry that the culprits could replicate it in other countries, since thousands of industrial plants all over the world rely on the same American-engineered computer systems that were compromised," *The New York Times* reported in a story about the incident.

These concerns extend to the electric utility industry, including power plants. "We tell our members that generation is a target for hacking, and we are seeing more cyber threats targeted to equipment in generation facilities," said Hollern, who is leading research to improve remote access security at generation plants.

In March 2018, the U.S. Department of Homeland Security (DHS) issued an alert warning of Russian government–sponsored cyber activity targeting the energy sector and other critical infrastructure sectors. In July, *POWER* reported on a DHS webinar indicating that Russian hackers infiltrated a power plant industrial control system. In addition, Hollern notes that there have now been five publicly reported cyber attacks on industrial facilities, starting with the Stuxnet attack in 2010.



These emerging threats come at a time when market pressures and digitalization have increased potential vulnerabilities of generation assets. As part of efforts to reduce operating costs, many utilities have moved plant personnel and monitoring tools to remote locations. New digital technologies have enabled these changes.

"Whether we like it or not, the electric sector is moving from analog to digital, and vendors are coming out with a lot of new digital technologies that are being incorporated into the control systems at power plants," said Hollern. "On one hand, this is a positive development because it increases automation and enables vendors and utilities to access plants remotely. But on the flip side, it creates a larger attack surface so that there is more opportunity to exploit vulnerabilities. We have to close those holes."

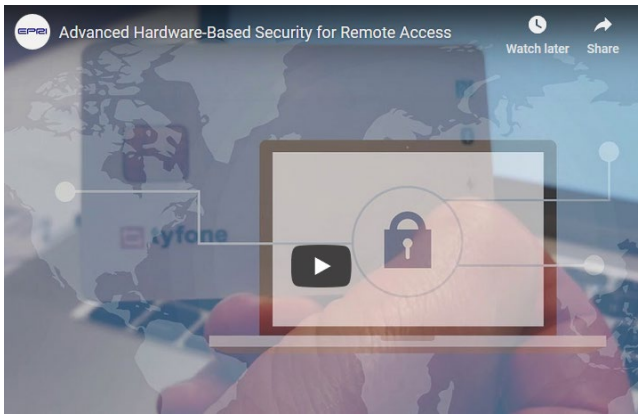
This is well recognized by the power industry. The North American Electric Reliability Corporation and DHS released guidance about implementing secure remote access of industrial control systems. EPRI recently led a collaborative project on cyber security solutions for instrumentation and control systems, with participation from more than 20 utilities. The group identified interactive remote access as its number one research priority, largely as a result of security concerns.

While increased use of digital technologies to remotely monitor and control generation facilities holds great promise for driving down costs and improving efficiency, a successful cyber attack can quickly erase those benefits.

DECENTRALIZED STORAGE OF KEYS

Electricity industry leaders are investing significant time and resources to bolster cyber security across the entire power system, including power generation, delivery, and distributed energy resources. In support of these efforts, EPRI is developing technologies and procedures to establish secure remote access to power plants. "Years ago, operators considered cyber security later in the plant design process and bolted on other technologies, processes, procedures, and personnel," said Hollern. "We are moving toward incorporating cyber security at the beginning of plant design and working with vendors and suppliers so that their products and services meet the cyber security requirements of the plant and utility upfront."

The aim of the three-year project, funded by EPRI's Technology Innovation program, is to help develop products that can achieve the highest level of remote access security as defined by the National Institute of Standards and Technology.



Watch a video about EPRI research on secure remote access for the electric power industry.

"The security level of remote access varies widely among generation facilities," said Hollern. "EPRI will offer tools and guides to help drive stronger, more consistent security measures across the industry."

The current approach to remote access of generation control systems typically involves issuing passwords and software tokens to users. These security "keys" are often stored in a centralized utility server, making the potential impact of a successful cyber attack more devastating.

"If someone were to hack into the network and steal the keys from the server, then you've lost all the keys issued to employees and vendors," said Hollern.

EPRI is examining an alternative in collaboration with Tyfone, Inc., an Oregon-based company that has developed digital security solutions for the banking and transportation sectors. The approach relies on decentralized storage of the keys along with physical identification cards. "We take all those keys out of the server and decentralize them," said Hollern. "Each key is stored on a card that can connect to computers through USB, Bluetooth, or near-field communication."

With this approach, a hacker that accesses a server won't be able to steal all the security keys at once. "If someone loses a card, you just de-provision that card," said Hollern. "You haven't lost all the keys to the kingdom."

Anti-tampering technology is built into the cards. "If you try to clone a card or take it apart, it will destroy itself," said Hollern. "It also uses multi-factor identification based on one-time passwords, long personal identification numbers, and biometrics—or a combination of all of those."

In addition, all remote connections require the approval of a supervisor at the time of connection. Supervisors receive requests on mobile devices and then decide whether to grant access.

"READY TO TAKE THE SYSTEM ON THE ROAD"

In 2016, EPRI completed the design of a decentralized, hardware-based remote access security system. Since then, researchers have been developing the cards and other remote access technologies for plant control systems, testing them at EPRI's Instrumentation and Controls laboratory in Charlotte, North Carolina, and incorporating lab results into a working prototype.

The initial results are encouraging. The security system achieved all its objectives:

- Securely store user data and security keys on smart cards
- Enable employees and vendors to securely access a plant's control systems from a corporate network and the cloud
- Interoperability with power plant infrastructure

EPRI has begun limited production of the cards and other technologies. "We have ironed out the bugs and are looking at potential new features to add," said Hollern. "We are ready to take the security system on the road and show utilities how it works. As part of this proof of concept, we will establish remote access to the EPRI lab."

In 2019, EPRI plans field tests in which utilities install the infrastructure and access control systems from different devices and using the cloud and corporate networks. These pilots may occur at fossil and nuclear power plants as well as in power delivery systems.

"The utilities will determine the specific applications," said Hollern. "They may decide to test the technologies on a non-production control system or monitoring system at first."

Feedback from these pilots will inform potential commercialization.

"We will make additional improvements based on how utilities issue cards and implement the technology in their networks," said Hollern.

Development of a commercialized product is expected to start by the end of 2019. "Remote access is essential as utilities transition more of their workforce away from plant sites," said Hollern. "This technology can help provide the security they need."

KEY EPRI TECHNICAL EXPERTS

Jason Hollern