Conference Panel Session

June 2024

TITLE:

DOE, EPRI, the DNP Users Group and Team - Taking OT Cybersecurity to the Next Level.

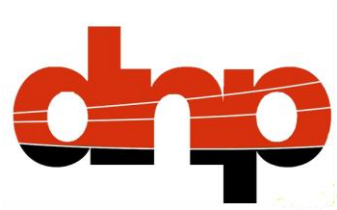
DESCRIPTION:

Meet and learn from the multidisciplinary expert team that are developing next generation OT cybersecurity technologies by building upon the work of the DNP Users Group. The goal of this team is to accelerate the completion and adoption of new OT cybersecurity standards thanks to the support of the US Department of Energy (DOE). The two resulting security technologies will address the challenges of the utility OT environment like no others.

The members of this panel session will discuss the DOE funded project from differing points of view, describing the technology and the project tasks including; complete the standards specifications; write test procedures; develop prototypes, code stack and test tools; perform interoperability testing and a utility demonstration.

The DER and SCADA environment is especially challenging for implementing security, consisting of mixed networks of both IP-based and serial networks which are typically low-bandwidth. The devices on these networks typically have limited processing power. SCADA networks are hierarchical, the serial portions lack a routing layer, and support limited access to accurate time synchronization. An issue with typical IT security solutions is that the authentication and encryption mechanisms do not reach the serial end devices. In addition, neither TLS nor IPSec are well-suited for low-bandwidth or low-processing-power environments.

Distributed Network Protocol Secure Authentication version 6 (DNP3-SAv6) and Authorization Management Protocol (AMP) are uniquely suited to solve the problems of securing devices in the DER and SCADA environments. These protocols use proven international cryptographic standards to provide end-to-end authentication, encryption, and access control for field devices that are not reachable by IP networks or do not have access to a utility's Certificate Authority. Important steps have been taken to support large field installations. Using DNP3-SAv6 and AMP, typical field staff can add devices to the secure network by authorizing certificates that are automatically created by the devices,



Conference Panel Session

without a human seeing the keys. SAv6 is included with the updated IEEE 1815™ (DNP3) standard, and AMP will become a new IEEE standard.

A key component of the security architecture is the AMP Authority which performs centralized authentication and authorization services. The AMP Authority integrates with the utilities' existing root Certificate Authority (CA) (Public Key Infrastructure) and acts as an intermediate CA for the SCADA system. In addition, the AMP authority can revoke credentials promptly without using a Certificate Revocation List (CRL).

Increasingly, utilities are connecting the control of their large DER sources to DERMS, ADMS and other systems using DNP3 (IEEE 1815) which is indicated in IEEE 1547-2018. Therefore, this project includes a focus on DER cybersecurity. Utilizing a testbed at EPRI's DER Integration Lab, the project includes integrating SAv6 and AMP within EPRI's Open Distributed Energy Resources Management System (OpenDERMS) and DER Gateway tools to evaluate the authentication, authorization, and key management controls. EPRI also intends to review SAv6 and AMP for alignment with IEEE 1547.3™ which is the IEEE guide for secure DER communications.

The DOE acceleration project also addresses essential components for wide industry adoption and multi-vendor interoperability including test procedures, code stack development, test tool development and multi-vendor interoperability testing.

The all-important final phase of the project consists of a multi-vendor utility demonstration at Salt River Project, who have been strong supporters of the DNP Users Group's cybersecurity program. Other commercialization related tasks are also planned.

The panel will be presented by EPRI, our utility partner, and our team of cybersecurity experts, most of whom serve on our Cybersecurity Task Force.