NIST SPECIAL PUBLICATION 1800-2A

Identity and Access Management

for Electric Utilities

Volume A:
Executive Summary

Jim McCarthy
National Cybersecurity Center of Excellence
Information Technology Laboratory

Don Faatz
Harry Perper
Chris Peloquin
John Wiltberger
The MITRE Corporation
McLean, VA

Leah Kauffman, Editor-in-Chief
National Cybersecurity Center of Excellence
Information Technology Laboratory

July 2018

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-2

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/es-idam-nist-sp1800-2-draft.pdf

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

Executive Summary

- The National Cybersecurity Center of Excellence (NCCoE) developed an example solution that electric utilities can use to more securely and efficiently manage access to the networked devices and facilities on which power generation, transmission, and distribution depend.
- The security characteristics in this access management platform are informed by guidance and best practices from standards organizations, including the North American Electric Reliability Corporation's (NERC's) Critical Infrastructure Protection (CIP) Version 5 standards.
- This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide uses commercially available products that can be included alongside your current products in your existing infrastructure. The integration of these products provides a converged view of all users within the electric utility's operational technology (OT) systems and information technology (IT) systems, as well as access to buildings and other facilities.
- The example solution is packaged as a "How-To" guide that demonstrates the implementation of standards-based cybersecurity technologies in the real world. The guide can help organizations to gain efficiencies in access management, while saving them research and proof-of-concept costs.

CHALLENGE

As the electric power industry upgrades infrastructure to adopt emerging technologies, utilities are also increasing OT and IT convergence. This allows more technologies, devices, and systems to connect to the grid to improve efficiency, provide access to data often held in silos, and enhance productivity.

This convergence challenges OT and IT departments to efficiently and effectively manage identities and access. Many utilities run identity and access management (IdAM) systems that are fragmented and controlled by numerous departments. Several negative outcomes can result: a lack of overall traceability and accountability regarding who has access to both critical and noncritical assets, an increased risk of attack and service disruption, and an inability to identify potential sources of a problem or attack.

To better protect power generation, transmission, and distribution, electric utilities need to be able to control and secure access to their resources, including OT systems, buildings, equipment, and IT systems. IdAM systems for these assets often exist in silos, and employees who manage these systems lack methods to effectively coordinate access to devices and facilities across these silos. This inefficient process can result in security risks for electric utilities, according to our electric sector stakeholders.

In collaboration with experts from the energy sector (mainly electric power companies) and those who provide equipment and services to them, we developed a scenario to describe a security challenge based on normal day-to-day business operations. The scenario centers on a utility technician with access to several substations and to remote terminal units that are connected to the utility's network in those substations. If the technician moves out of the region and resigns, a consolidated IdAM system can quickly and consistently remove the technician's access to all facilities and systems. This provides the timely management of access and reduces the potential for errors. Electric utilities need this ability to provide the right person with the right degree of access to the right resources at the right time.

SOLUTION

To help the energy sector address this challenge, we developed an example solution that electric utilities can use to more securely and efficiently manage access to the networked devices and facilities on which power generation, transmission, and distribution depend. Our solution uses commercially available products to demonstrate a converged IdAM platform, providing a comprehensive view of users across all of the entity's business and utility operations silos, and the access rights granted to those users. This platform is described in this NIST cybersecurity *Identity and Access Management* practice guide.

Electric utilities can use some or all of the guide to implement a converged IdAM system by referencing related NIST guidance and industry standards, including NERC CIP Version 5. Commercial, standards-based products, like the ones that we used, are easily available and interoperable with commonly used IT infrastructure and investments. In our lab at the NCCoE, which is part of NIST, we built an environment that simulates an electric utility's architecture. This architecture includes the typical technology silos found in a utility (such as operational technology, IT, and physical access control systems).

The practice guide includes three versions of an end-to-end identity management solution that provides access control capabilities to reduce opportunities for cyber attack or human error. It accounts for the risks that converged control can present. In this guide, we show how an electric utility can implement a converged IdAM platform, using multiple commercially available products, to provide a comprehensive view of all users within the electric utility, across all silos, and of the access rights that they have been granted.

The guide:

- maps security characteristics to guidance and best practices from NIST and other standards organizations, including NERC CIP Version 5 standards
- provides a detailed example solution with capabilities that address security controls, and demonstrates a modular approach that uses different products to achieve the same results
- includes instructions for implementers and security engineers, including examples of all of the necessary components and installation, configuration, and integration
- uses products that are readily available and interoperable with your existing IT infrastructure and investments
- can meet the needs of electric utilities of all sizes, including corporate and regional business offices, power generation plants, and substations

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

BENEFITS

The NCCoE's practice guide to *Identity and Access Management for Electric Utilities* can help your organization:

- adopt products and capabilities on a component-by-component basis, or as a whole, thereby minimizing impact to the enterprise and existing infrastructure
- reduce the risk of malicious or untrained people gaining unauthorized access to critical infrastructure components and interfering with their operation, thereby lowering the overall business risk
- allow for rapid provisioning and de-provisioning of access from a converged platform, so that personnel can spend more time on other critical tasks
- improve situational awareness: proper access and authorization can be confirmed through the use of a single, converged solution
- improve the security posture by tracking and auditing access requests and other IdAM activity across all networks
- enhance the productivity of employees and speed delivery of services, and support oversight of resources

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/use-cases/idam. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at energy_nccoe@nist.gov.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

LEARN MORE
Visit https://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200