CLEAN ENERGY CYBERSECURITY ACCELERATOR

Clean Energy Cybersecurity Accelerator Cohort 1:

Authentication and Authorization

2023

Jake Beley, Nicholas Blair, Jennifer Guerra, Adarsh Hasandka, Chelsea Quilling, Anthony Wallace, Katherine Amoresano, Wendy Folger, and Gareth Williams

National Renewable Energy Laboratory

CECA Contributors

CECA Technical Assistance
Glatter, Casey
Singh, Vivek Kumar

IEC Program Management
Brubaker, Ryan
Mujumdar, Monali

Patria Security
Richardson, Bryan
Schwalm, Keith

Cyber Range Assistance
Abbondanza, Michael

Report Production and Editorial Assistance
NREL Communications and Public Affairs personnel

Technical Advisors
Granda, Steve
Henry, Jordan
White, Jonathan

Acknowledgments

The authors thank the U.S. Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and the Office of Energy Efficiency and Renewable Energy (EERE) for supporting this effort. In addition, we thank utility industry partners Berkshire Hathaway Energy, Duke Energy, and Xcel Energy for sponsoring the technical assessments.

Cohort 1 Solution Providers:

BlueRidge Networks

Binary Armor, Sierra Nevada Corporation

xage Security

Sponsors:

U.S. Department of Energy

U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response

U.S. Department of Energy, Office of Energy Efficiency & Renewable Energy

Berkshire Hathaway Energy

Duke Energy

Xcel Energy

Managed by:

NREL, Transforming Energy

Notice

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

National Renewable Energy Laboratory
15013 Denver West Parkway, Golden, CO 80401
303-275-3000 • www.nrel.gov

NREL/TP-5R00-86205 • September 2023

NREL prints on paper that contains recycled content.

Table of Contents

Overview

Mitigating risk in an evolving electric grid will require rapid innovation and deployment of cybersecurity technologies for the energy sector and appropriate applications of existing technologies. The mission of the Clean Energy Cybersecurity Accelerator™ (CECA) is to bolster the security of the U.S. electric grid by fostering the development of emerging technologies that outpace evolving threats.

In the 2023 National Cybersecurity Strategy, the Biden-Harris Administration defines the need for a "defensible, resilient digital ecosystem where it is costlier to attack systems than defend them" (The White House 2023). CECA's efforts help secure future clean energy technologies by bridging the capabilities of private industry and the cybersecurity needs of utility customers.

CECA is a partnership among the U.S. Department of Energy (DOE), the National Renewable Energy Laboratory (NREL), utilities, and solution providers. A utility working group sponsors NREL to use its grid simulation environment to evaluate the efficacy of different innovative cybersecurity technologies, referred to as solutions. These evaluations are conducted in a series of six-month cohorts, each centered around a "theme." Themes are based on threats defined and prioritized by CECA's utility partners. Based on the results of that analysis, each cohort is prepared to emulate threats and test mitigations with the highest security payoff for the evolving grid. Cohort 1's theme centered on authentication and authorization. Future cohort themes will address a wide range of industrial control system (ICS) cybersecurity challenges facing the future electric grid based on the most pressing cybersecurity challenges facing utilities and DOE partners.

Once selected for a CECA cohort, solution provider technologies undergo evaluations across several realistic threat scenarios in a live operating environment that is representative of the utilities' infrastructure. CECA technical reports offered detailed and quantifiable results to each solution provider, highlighting where solutions successfully prevented attacks and noting opportunities for improvement. This report (and future public reports) is intended to provide a high-level overview of the program, an introduction to the cohort theme, a description of solution provider participants, the technical approach to CECA evaluations, and key security takeaways.

Cybersecurity is a never-ending fight. Threats, architectures, and technologies will continue to evolve as the energy sector undergoes significant transformations. Utilities face complex challenges in managing risks to the modern electric grid. CECA is designed to ensure that utility sponsors have a primary voice in prioritizing which cybersecurity gap or threat is addressed by each cohort's effort.

Cohort 1: Authentication and Authorization

Cohort 1 of CECA launched in the fall of 2022 with a focus on solutions that provide authentication and authorization for ICS to mitigate attacks on the electric grid. Authentication

and authorization verify that the identity (authentication) and permissions (authorization) of a user or a device align with their assigned roles. The exploitation of weak authentication and authorization controls can lead to malicious actors gaining access and privilege to critical devices, systems, and information, and it can impact system operations. Improved authentication and authorization offer benefits across the energy sector, with particular benefits for clean energy technologies, which demand enhanced connectivity due to their distributed nature.

Utility partners, in conversations with NREL, defined the theme covered within Cohort 1. The theme then determined the limits to the scope of the cohort. The utilities also collaborated with CECA to determine the experiment environment most appropriate for evaluating the theme as well as the solutions to be tested. NREL informed this choice by advising on several aspects of the environment and ensuring that the chosen environment was compatible with the Advanced Research on Integrated Energy Systems (ARIES) Cyber Range (NREL n.d.).[1] CECA program funding, and Cohort 1's timeline. Future cohorts might vary in several aspects, most notably in the theme and solution providers; however, the program's structure will continue to prioritize collaborative engagement with utilities and rigorous evaluations to advance the cybersecurity posture of critical energy networks. To assess the strength of Cohort 1's solutions, CECA devised threat scenarios grounded in historical precedent. The CECA team leveraged exploit techniques from real-world case studies of state-sponsored actors to develop the assessment's attack paths and targets.

Not all CECA cohort evaluations directly, let alone exclusively, address clean energy cybersecurity. The purpose of the CECA program is to accelerate the adoption of highly effective cybersecurity for the clean energy-driven future electric grid, its operators, and the public it serves. The architecture used for the Cohort 1 assessments, as defined by utility partners, did not include a clean energy component. Cohort 1 provides a solid foundation for the incorporation of clean energy technologies in future cohorts of CECA. Authentication and authorization are evergreen challenges affecting ICS environments regardless of the specific operational technologies deployed. Further, utility partners selected the experiment environment they felt best addressed their needs. Given the scope of the selected emulation environment, neither the threat emulation scenarios nor the results of the evaluations for Cohort 1 would have changed had clean energy technologies been included.

CECA Cohort 1 produced three technical reports—one for each solution provider—summarizing the evaluation environment and results of the Cohort 1 assessments for each solution. The solution provider technical reports are private to each solution provider and the program sponsors, as defined by the multiparty nondisclosure agreements. This report summarizes all findings from Cohort 1.

[1] https://www.nrel.gov/security-resilience/cyber-range.html

Cohort 1 results provided the energy industry, solution providers, and related agencies with valuable insights into the efficacy and applicability of solutions in common system configurations under realistic threat scenarios. The results of the assessment highlight areas of future exploration and analysis in subsequent technology iterations.

Solution Providers

With Cohort 1's theme defined, on June 6, 2022, CECA released a public call for applications from solution providers offering methodologies to mitigate challenges related to authentication and authorization. NREL experts and utility partners collaboratively reviewed and selected applications for Cohort 1. Products proposed by the applicants offered a range of innovative methods to authenticate and authorize users and devices to ICS networks, from the physical layer to the application layer. A public call for future applications will be published on the CECA website at the launch of each new cohort.

Three solution providers were selected to participate in Cohort 1: Blue Ridge Networks, Sierra Nevada Corporation, and Xage Security. Each participating company described their solution(s).

Blue Ridge Networks

Blue Ridge Networks' LinkGuard™ solution applies CyberCloak™ capabilities to isolate, conceal, contain, and encrypt critical network assets and operations to prevent discovery and data exfiltration. The deployment of LinkGuard components can be tailored to protect a wide variety of use cases with minimal integration to reduce the protected attack surface. LinkGuard was chosen for Cohort 1 because its secure enclave features provide authentication to the LinkGuard devices and software connecting to the enclave. Cohort 1's assessment focused on the LinkGuard Management System, LinkGuard hub controller (BorderGuard), and LinkGuard deployed gateways (RemoteLink).

LinkGuard provides an independent protocol-agnostic private network overlaid on existing network infrastructure, including public networks, to create secure network enclaves without impacts or dependencies on existing network Internet Protocol (IP) addressing. The secure enclave is established, or extended, by deploying LinkGuard RemoteLink devices or software. Hosts on the private side of those LinkGuard components, which are inside a given enclave, are trusted to communicate with other LinkGuard hosts in the secure enclave but are inaccessible by hosts on the public side of these devices, which are outside a given enclave.

LinkGuard CyberCloak capabilities are compatible with other defenses to support a robust, multilayer, defense-in-depth cybersecurity architecture.

Sierra Nevada Corporation

Sierra Nevada Corporation's Binary Armor® is designed to protect machine-to-machine communications against cyberattacks, insider threats, and operator error. Binary Armor was selected for Cohort 1 because of its authorization and communication security features that

improve operational control, provide greater command assurance, and secure the bridge between information technology (IT) and operational technology (OT) networks. These features enable administrators to capture and analyze information on regular network traffic and anomalous events within critical networks.

Binary Armor provides ICS-native deep packet inspection to enforce authorization. The solution evaluates each byte of every message sent to and from substations to prevent dangerous commands from reaching assets. Finally, Binary Armor allows administrators to create detailed firewall rules to allow only specific devices and protocols to communicate with critical ICS assets (Binary Armor n.d.).

Xage Security

Xage Security provides a resilient cybersecurity mesh platform that defends OT and IT assets. Xage's core technology, Xage Fabric, enables identity-based access control, remote access, and data exchange in OT and IT networks. The Fabric is overlaid on existing OT and IT networks by installing Fabric Nodes, usually as virtual machines, without requiring hardware replacements, software agents, or disruptive network architecture changes. Xage also offers an optional bump-in-the-wire device, the Xage Enforcement Point (XEP), which can control access down to the level of individual assets, such as remote terminal units and programmable logic controllers. Xage controls user-to-machine, application-to-machine, and machine-to-machine access, proactively preventing attacker lateral movement.

Xage offers a browser-based interface to create granular, identity-based policies for access control, enforcing the principle of least privilege and providing just-in-time, just-enough access to operators and technicians to access protected OT devices. End users access assets through the in-browser console. Policies are centrally created, then distributed among Fabric Nodes and XEPs, which locally enforce them at distributed operational sites. Xage Security was chosen for Cohort 1 based on its authentication and authorization capabilities that implement multifactor authentication, provide single sign-on identity management, and control uni- and bidirectional data flow.

Xage also relies on distributed ledger technology to ensure the resilience, integrity, and availability of the Fabric. The Xage Fabric allows each node to maintain a locally updated chain of configurations and changes to help ensure system integrity. Xage uses data fingerprinting, Internet Protocol Security (IPSec) tunnels, strong encryption, and granular access control to ensure the confidentiality, integrity, and authenticity of data being moved through the Fabric.

NREL Cyber Range: Scope and Evaluation Environment

Cohort participant solutions were tested on the NREL ARIES Cyber Range, a scalable cyber-physical environment used for controlled threat emulation. The ARIES Cyber Range provides rich visualization and data collection capabilities for users to directly interact with a live high-fidelity network.

Scope

In Cohort 1, NREL researchers analyzed how the selected solution providers' authentication and authorization mechanisms performed against some of the tactics used by advanced adversaries. The engineers and solution providers determined the appropriate experimental configuration within the ARIES Cyber Range using the bounds of both the assessment timeline and the prioritized threat. The cohort scope did not include a security assessment of the products (e.g., penetration testing, physical access threat scenarios, or other means of impacting or exploiting these products). The scope was limited to an assessment of the authorization and authentication features of the participant solutions.

Evaluation Environment

Cohort 1 solutions were tested under a common operating environment. The environment emulated a small-scale version of a realistic electric distribution grid that included power system simulation, an enterprise network, multiple substations, and a utility control center (Figure 1). This environment was created and mutually agreed upon by NREL technical experts and utility partners. To represent the electric distribution grid, engineers selected a simplified microgrid model that included various ICS devices and bidirectional communications using a realistic supervisory control and data acquisition (SCADA) architecture.

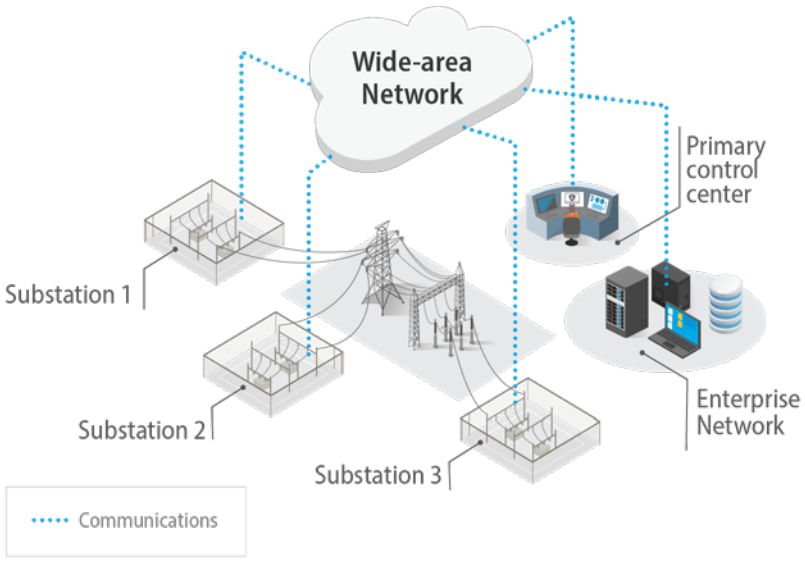

Figure 1: Cohort 1 simulated evaluation environment. *Illustration by NREL*

Threat Scenarios

The CECA Threat Emulation Team based the evaluation plan on previously observed ICS attacks. CECA neither deployed malware nor performed penetration testing in Cohort 1. NREL experts,

in coordination with solution providers, selected 16 techniques across 8 tactics found within the MITRE ATT&CK for ICS framework that can be mitigated by authentication and authorization.

The MITRE ATT&CK framework is a widely used, publicly available resource to classify and categorize real-world adversary activity into tactics that represent the phases of a cyber kill chain and specific techniques that adversaries have used to accomplish each of those tactics. MITRE maintains three separate matrices—mobile, enterprise, and ICS—that are based on threats observed in that domain. CECA specifically used the ICS matrix to categorize testing procedures.[2] MITRE ATT&CK for ICS was created to better understand attacker behavior and to provide a holistic view of adversarial tactics, techniques, and procedures in the ICS domain (Alexander, Belisle, and Steele 2020).

To scope the assessment, the CECA team identified techniques that could be mitigated by strong authentication and authorization solutions. The CECA team further narrowed the list to include only techniques that most solution providers applying to participate in Cohort 1 claimed to mitigate.

Figure 2 displays the MITRE techniques selected for this cohort. CECA grouped these techniques to create six threat scenarios representing specific phases or situations of an ICS cyberattack. Each scenario implemented two or more techniques in the form of procedures.

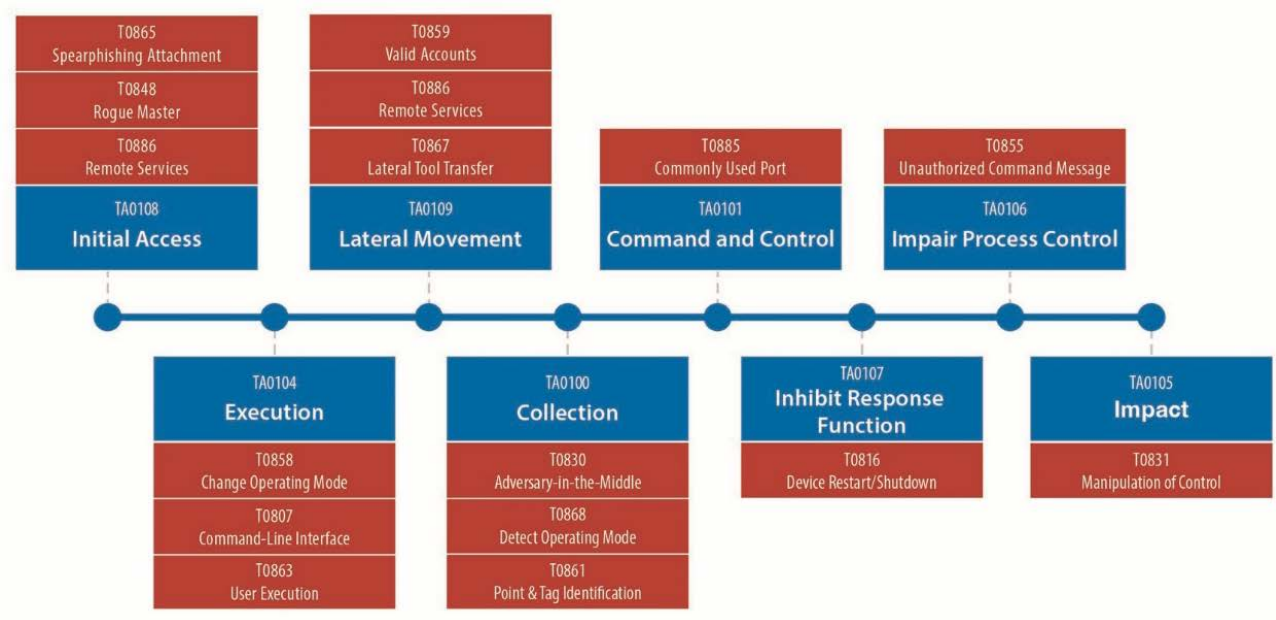

Figure 2: MITRE ATT&CK tactics (blue) and techniques (red) used in the Cohort 1 threat scenarios. *Illustration by NREL*

[2] https://attack.mitre.org/matrices/ics/

Finally, with this select list of tactics and techniques, CECA created attack scenarios. CECA evaluated whether each authentication and authorization solution prevented or did not prevent the attack. Cohort 1's evaluation approach using MITRE ATT&CK for ICS was approved by utility partners to provide a standardized framework for analyzing the results of CECA tests. While the CECA evaluation did not deploy malware, the emulations were generally representative of recent ICS cyberattacks, some of which are indicated in the below summary of CECA Cohort 1's threat scenarios:

End-to-End Kill Chain: CECA Cohort 1 threat scenarios 1 and 2 represented an end-to-end kill chain of an advanced persistent threat. Threat scenario 1 tested the initial access phase, and threat scenario 2 represented multiple malicious effects once an attacker gained access to a control center. Threat scenarios 1 and 2 are particularly timely given the recent discovery of the malware named PIPEDREAM, as characterized by Brubaker et al. (2022), which contains modules to execute an entire end-to-end ICS attack. The adversary can use this single malware to run every aspect of the kill chain, including command and control, sending vendor-specific malicious ICS commands, and pivoting from the enterprise network to the ICS network (Brubaker et al. 2022).

Point of Presence on Substation Network: Threat scenario 3 emulated an adversary who was able to gain a point of presence on a substation network and attempted to conduct malicious activity. This attack method has been primarily observed in situations where radio equipment was used to target substations or SCADA devices to gain a point of presence in the SCADA network (Abrams and Weiss 2008; Bastille 2017). However, there are many ways an attacker can gain a point of presence on a substation network, including an insider threat or an insecure Wi-Fi access point. Threat scenario 3 evaluates whether attackers who have gained this access are forced to authenticate before they can issue commands.

Point of Presence on Control Center Network: Threat scenarios 4, 5, and 6 showcased an attacker with access to the control center network. Threat scenarios 4 and 5 tested an attacker's ability to collect valid credentials from insecure communications and then use those credentials to access OT assets. There have been proofs of concept of this type of credential collection in ICS protocols (SANS ICS 2021), and similar spoofing to access OT assets was observed in the Maroochy Shire water service attack in 2000 (Abrams and Weiss 2008). In threat scenario 6 the attacker attempted to intercept and modify traffic flowing between the substations and the control center, which was inspired by the capabilities found in the VPNFilter malware designed to infect network infrastructure (Largent 2018a; Largent 2018b; S4 Events 2019).

Conclusions

Cohort 1 paved the way for the CECA program and proved the importance of cybersecurity technology assessments under realistic threat scenarios, in a representational environment. In

the domains of authorization and authentication, this cohort tested how several innovative security technologies perform against realistic attacks. Several key challenges learned during Cohort 1 assessments are summarized next, followed key takeaways, and cybersecurity considerations for future clean energy technologies.

Key Cybersecurity Challenges Identified

Challenges Related to Security Definitions

CECA's coordination with solution providers highlighted a key challenge facing utilities—that the language used by solution providers to market their products is often misaligned with utility customer expectations and definitions of common security terms. For example, CECA's technical team experienced this first-hand in the variety of ways solution providers defined "zero trust." Many solution providers in the industry market their products as implementing a zero-trust approach; however, there are conflicting ideas on what zero trust entails, leaving utilities with challenges in determining whether or how security solutions are protecting and securing their assets and networks. Conflicting terms and definitions demonstrate that cybersecurity solutions marketed to protecting utility networks are still maturing. While this immaturity lends itself to opportunities for innovation and competition, it can also lead to confusion and overpromises that do not provide the security and protection utilities are seeking.

Challenges of ICS Assessments

Undertaking threat emulation and assessments like those developed by CECA experts is difficult because of the lack of publicly available threat intelligence specific to ICS. Leveraging existing threat intelligence sources like the MITRE ATT&CK for ICS framework and the Electricity Information Sharing and Analysis Center (NERC n.d.) is vital in creating actionable procedures to protect infrastructure moving forward. Increased threat sharing and visibility into critical infrastructure cyberattacks would accelerate research in ICS defense and enable additional accuracy of threat emulation for improved security mitigation. Threat information that is shared responsibly and in an anonymized manner does not need to be exactly replicated to gain important insights or add value to industry partners working to defend critical networks.

Challenges of Device-to-Device Authentication

The results of the threat emulation scenarios highlighted that device-to-device authentication is a difficult problem, particularly in OT portions of utility networks. In one threat scenario where an attacker-in-the-middle sought to alter data flowing between devices, CECA found that solutions were unable to prevent the attacker from manipulating the control center's view of the system by strategically changing data values before they reached the control center. In some test cases, deploying a solution differently may have prevented the attacker from achieving their aims, but in most cases an attacker would have been successful regardless of where the solution was deployed. To solve this problem, solution providers need to add

integrity checks to critical data flows to validate that the data received by a device has not been manipulated.

Key Takeaways From Threat Scenario Results

Cohort 1's examination of authorization and authentication in an OT environment highlighted four key security principles:

Move Beyond Perimeter Security: The first security principle revealed in Cohort 1 assessments is the importance of designing systems that presume a security breach will occur. Scenarios 1 and 2 reinforced the value of defense-in-depth to mitigate the damage of a breach. Security approaches that focus heavily on perimeter security will continue to fail in modern, hyper-connected systems. Scenarios 1 and 2 also demonstrated the importance of assuming breaches will occur and moving authentication mechanisms to devices within critical network segments. These scenarios also emphasized the importance of using multifactor authentication to defend against an attacker's lateral movements through a compromised network. Passwords may be easily recovered by an adversary with even a small foothold in a network, but multifactor authentication can add a critical layer of additional security to authentication systems.

Cyber Security Insight

Design systems and security assuming a breach.

Security Device Placement Enhances Visibility: The second security principle that Cohort 1 uncovered from the assessment is the importance of device placement to enhance network visibility. In threat scenario 3, several tests showed where a solution included a feature that could have prevented an attack but was unable to do so because of its placement of the solution within the OT network. Security solutions should be placed as close as possible to the assets they are deployed to protect.

Cyber Security Insight

Place devices strategically to maximize security features.

Signature-Based Detection Methods Have Limitations: The third security principle demonstrated by Cohort 1 is that signature-based detections alone are not enough to defend networks. Scenarios 4, 5, and 6 demonstrated that defensive solutions that depend on preconfigured-allowlisting are vulnerable to "living off the land" techniques in which adversaries leverage legitimate device relationships and functionality within a control system environment to perform malicious activity. These kinds of attacks are particularly insidious and demonstrate the importance of performing authentication and authorization checks at multiple points within the network.

Cyber Security Insight

Perform authentication at multiple points within a network.

Inspecting Multiple Network Layers Enhances Awareness of Data Flows: The fourth security principle uncovered in Cohort 1 is that solutions should inspect multiple layers of the network to provide the best authentication and authorization protection. Scenarios 2 and 4 demonstrated the value protections that extend beyond the application layer. A solution or a combination of solutions that can look at multiple layers of the Open Systems Interconnection model, such as the application and network layer, help protect against a wider set of attacks.

Cyber Security Insight

Deploy solutions that inspect multiple network layers.

Future Technologies for Clean Energy

The expansion and adoption of distributed energy resources will further intensify the need for authentication and authorization solutions. Current technological advancements are enabling more robust network topologies to underpin ICS/SCADA networks. For example, future networks, which include high penetrations of distributed energy resources implemented closer to the home, and in some cases within the home, will provide more data and visibility than ever before. This movement toward the consumer must include secure device-to-device relationships that protect the privacy of customers and the operational integrity of equipment. Using secure authentication and authorization solutions can significantly reduce the attack surface of the evolving grid.

References

Abrams, Marshall, and Joe Weiss. 2008. "Malicious Control System Cyber Security Attack Case Study—Maroochy Water Services, Australia." McLean, VA: The MITRE Corporation. Case #08-1145. https://www.mitre.org/sites/default/files/pdf/08_1145.pdf.

Alexander, Otis, Misha Belisle, and Jacob Steele. 2020. *MITRE ATT&CK for Industrial Control Systems: Design and Philosophy*. McLean, VA: The MITRE Corporation. Project No.: 01ADM105-OT. https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf.

Bastille. 2017. "Dallas Siren Attack." April 17, 2017. https://www.bastille.net/blogs/2017/4/17/dallas-siren-attack.

Binary Armor. No date. "What Can Binary Armor OT Cybersecurity Do for You?" Accessed April 20, 2023. https://binaryarmor.com.

Brubaker, Nathan, Keith Lunden, Ken Proska, Muhammad Umair, Daniel Kapellmann Zafra, Corey Hildebrandt, and Rob Caldwell. 2022. "State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems." Mandiant. April 13, 2022. Last updated December 2, 2022. https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool.

Largent, William. 2018a. "New VPNFilter Malware Targets at Least 500K Networking Devices Worldwide." Cisco Talos Intelligence Blog. May 23, 2018. https://blog.talosintelligence.com/vpnfilter/.

Largent, William. 2018b. "VPNFilter Update—VPNFilter Exploits Endpoints, Targets New Devices." Cisco Talos Intelligence Blog. June 6, 2018.https://blog.talosintelligence.com/vpnfilter-update/.

Mathezer, Stephen. 2021. "Introduction to ICS Security Part 3: Remote Access Best Practices." SANS Institute. October 1, 2021. https://www.sans.org/blog/introduction-to-ics-security-part-3/.

National Renewable Energy Laboratory (NREL). No date. "NREL Cyber Range." Accessed March 1, 2022. https://www.nrel.gov/security-resilience/cyber-range.html.

North American Electric Reliability Corporation (NERC). No date. "Electricity Information Sharing and Analysis Center." https://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx. Accessed April 20, 2023.

Rose, Scott, Oliver Borchert, Stu Mitchell, and Sean Connelly. 2020. *NIST Special Publication 800-207: Zero Trust Architecture*. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207.

S4 Events. 2019. “VPNFilter Deep Dive.” YouTube. https://www.youtube.com/watch?v=yuZazP22rpI.

SANS ICS. 2021. “Modbus Man-in-the-Middle.” YouTube. https://www.youtube.com/watch?v=-1WbegoU8i0.

The White House. 2023. National Cybersecurity Strategy. Washington, D.C. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.