DNP Users Group Workshop Series

Trends in Technologies for OT Cybersecurity

Identifying and Addressing Gaps with Conventional/Common Cybersecurity Methods

Thursday, October 31, 2024, 3:00 - 4:30 PM ET

The workshop notes and recording are offered at no charge to our members and non-members.

Post Event Release

Video Recording

See below for Chat Notes and Reference Information

Description

The DNP Users Group (DNP-UG) is launching a series of informative workshops, open to the public, with industry leaders addressing important topics relevant to our members and the industry. Workshops will generally be followed by related tutorials and training courses for our members.

OT cybersecurity is an area that is receiving increased attention with a growing consensus that vulnerabilities exist that must be addressed. However, numerous challenges make achieving comprehensive defense-in-depth OT cybersecurity in mixed networks of IP and serial communications difficult if not unlikely, especially considering the many other priorities utilities face. In addition, typical IT security solutions do not address the requirements of the SCADA environment. Significant efforts are underway to develop new standards that will address many of the unique requirements of OT cybersecurity and facilitate broad adoption.

This panel featured five industry leaders discussing design, engineering, standards and technology approaches. Our speakers are from DHS CISA, Idaho National Labs, EPRI, Xanthus Consulting and the DNP Users Group.

Topics included secure communications, Secure by Design, zero trust for OT, Cyber Informed Engineering, DOE supply chain cybersecurity principles, SBOMs to enhance security, vulnerability testing for OT, key threats, challenges in deploying OT security, DOE, UL, IEEE standards, DER and IBR cybersecurity, gaps with conventional/common methods, unique aspects of the pending SAv6 & AMP standards including, novel enrollment methods and steps toward zero trust architecture.

Ample time was allotted for audience participation and discussion.

Speakers

- John McDonald, Panel Chair, JDM Associates
- Matthew Rogers, DHS CISA
- Ginger Wright, Idaho National Labs
- Ben Sooter, EPRI
- Frances Cleveland, Xanthus Consulting
- Grant Gilchrist, DNP Users Group, Tesco Automation

To receive periodic updates and news, click here: **Enroll**

The DNP-UG is a non-profit group with the mission to actively support measures to improve interoperability and cybersecurity in DNP systems by developing technologies and standards, implementing a conformance program, and providing education to the industry. Utilities and vendors benefit significantly with reduced project and development costs and risks due to a broadly adopted, well managed, highly interoperable and secure protocol (if implemented).

To participate and support our work please join us! Click here: **Membership Guide** or **Join**

For more information click here: **dnp.org home**

Follow us on **LinkedIn**

For assistance or more information, contact us at dnpusers.membership@gmail.com

Speaker Pictures and Short Bios – refer to the Info and Details document **here.**

Workshop Chat Notes

1. **How widely is DNP secure used in the utility space?**
   - Response from Grant Gilchrist: [Version 6] of the standard is still in development. DNP3-SAv5, the earlier version, has been used in a few good-sized projects but generally there hasn't been enough push from the utilities to say they want it.
   - Response from Frances Cleveland: DNP3 is used by virtually all utility SCADA systems for management of their grids.
   - Comment from Frances Cleveland: In terms of protocols for DER communications, a critical cybersecurity issue in DER is that most DER systems use Modbus for communications - Modbus has no cybersecurity! That is one reason we are hoping that DNP3 with its security will be used more extensively in the DER world.
   - Response from Grant Gilchrist: I will point out that SAv6 and AMP can in theory be used with Modbus if vendors want to do that.
   - Response from DNP-UG: Responses to a recent Evans-Newton survey indicated that DNP3 is used by about 94% of North American electric utilities.
   - Response from DNP-UG: DNP3 documentation uses the terms “Secure Authentication” and “DNP3-SA” to refer to the cybersecurity functions discussed here. “DNP3-SAvX” or “SAvX” are used when necessary to distinguish a specific version of DNP3-SA [i.e. version X]. A number of books and academic papers have used the terms “DNP Secure” or “DNPSec” to discuss various mechanisms to provide cybersecurity features for DNP3. Typically, these are not referring to DNP3-SA.
2. **Who is managing CA for DNP3 SA?**
   - Response from Grant Gilchrist: In DNP3-SAv6, the idea is that all devices manage their own credentials, but a central authority gets to decide who can talk to whom. AMP can be used either with the AMP Authority acting as a CA, or as an Intermediate Authority within a utility’s Key Infrastructure.
3. **Could you tell us again what AMP stands for?**
   - Response from Grant Gilchrist: Authorization Management Protocol
4. **Is Open SSL certs secure, like self signed for Client-Server communication?**
   - Response from Grant Gilchrist: AMP and DNP3-SAv6 are designed to be able to start with self-certified communications and then upgrade each comms link to authority-signed certificates.

5. **I still see a lot of people who believe that their systems are not widely known and there is "security by obscurity". On a scale of 1 to 10, how wrong do you think they are?**
    - Response from Matthew Rogers: 10
    - Response from Grant Gilchrist: Can I take this one up to 11? We lost that ability the first time we connected a control center to the corporate network, firewall or no.
    - Response from Virginia Wright: I think that has become a 10! We can use search engines to draw engineering information from job listings or even small procurement documents that may help an adversary in their quest to do harm. We now have automation that can spend every moment of every day testing potential attack concepts against a system and learning from the attempts. Security by Obscurity is unfortunately an antique concept.
    - Response from Grant Gilchrist: The government is taking this even further with the zero-trust initiative. Every device needs to be doing authentication.
6. **What's the state of understanding of nation state insider threats who may be trusted operators of critical infrastructure? Identification, monitoring, background checks, compensating controls?**
    - Response from Matthew Rogers: This is a great graphic from ODNI on some of these low-level threat actors hacking low hanging fruit in critical infrastructure https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf
    - Response from Virginia Wright to Everyone: Great question! There is rising awareness that the supply chain for critical infrastructure doesn't become resolved at the time of procurement and delivery. Increasingly vendors and integrators are key partners in operation, and that means that they are part of the core security envelope for a system. Insider threats are one element to consider and also the vendor / integrator as watering hole. We mentioned some good techniques for mitigating insider threats.
    - Response from Frances Cleveland: There will always be successful cyber-attacks, from the inside and outside, so compensating controls, Plan Bs, are critical. The NIST Cybersecurity Framework is an excellent source of seeing how to understand all the cyber issues.
7. **Does next-gen DNP3 protocol need to consider adopting PQC algorithm against future quantum computing attacks?**

- Response from Frances Cleveland: Quantum computing and quantum security is one of the areas that the IEC and IEEE are looking at — not that we yet know how best to deal with this new technology.
- Comment from DNP-UG: DNP3-SAv6 is designed to accommodate post-quantum cryptography in the Association handshake (the opening of authorized communication between a pair of devices) and already relies on quantum-safe symmetric cryptography for its Session handshake and for message authentication and encryption (the on-going traffic between those devices).

8. **As an equipment manufacturer for an embedded device (Power Quality Analyzer). Which Standard would you recommend certifying against — IEC 62443-4-2 or ISO 270001 (or perhaps a different one!)?**
    - Audience comment from Stephen Trachian: IEC 62443-4-2 would be my recommendation.
    - Response from Frances Cleveland: ISO 27001 is high level. IEC 62443-4-2 is far more detailed. The IEC also has the IEC 62351 series on many issues — specifically HOW to solve the problems, not just WHAT needs to be done. For example IEC 62351-8 specifies HOW to do Role-Based Access Control (RBAC).
    - Audience comment from Andrew West: If you only talk to IT, ISO 27001 is fine. If you plug into an industrial system (hint: Power Quality Analyzer...), IEC 62443 is a better choice. There may also be regulatory requirements (which don't always align with technical best practice).
    - Response from Grant Gilchrist: Refer to Guidelines for Smart Grid Cybersecurity (NIST IR 7628)
    - Response from the DNP-UG: We plan to provide conformance certification services as part of our Conformance Certification Program, once the standards and test procedures are completed.
9. **Would data diodes effective in OT security?**
    - Audience comment from Andrew West: Data diodes are great if you have a one-way information flow. By definition, SCADA is bidirectional...
    - Response from Frances Cleveland: Data diodes can be useful, but often one-way data flows end up being difficult to maintain if you really want a conversation.
10. **IEEE 2030.5 has Smart Energy Root CA (SERCA), how about DNP3 SA case?**
    - Response from Grant Gilchrist: There is not a single root CA defined for DNP3 security. The assumption has been that the utility would prefer to have their own CA and PKI.

- Response from Frances Cleveland: We are discussing having groups of CAs that can extend the reach of utilities out to the thousands of DERs

11. **Does CISA plan to develop any standard that will require software development companies to have security embedded in their code, similar to FedRAMP program?**
    - Response from Matthew Rogers: This exists to some degree with the Secure Software Development Attestation form https://www.cisa.gov/secure-software-attestation-form and https://www.cisa.gov/securebydesign/pledge Additionally, we just released an RFI for Software Bad Practices, things that would be considered negligent in software development. CISA and FBI Release Updated Guidance on Product Security Bad Practices | CISA
    - Response from Virginia Wright: DOE CESER Supply Chain Principles: https://www.energy.gov/ceser/supply-chain-cybersecurity-principles and https://cytrics.inl.gov/
    - Response from Frances Cleveland:DOE/ NARUC cybersecurity baselines for distribution system operations and DER are at https://pubs.naruc.org/pub/35247A70-0C45-9652-C6D9-99A77C87200F
12. **What are the thoughts on new devices that come installed with embedded web pages? My instinct is to switch these off and remove the risk - but can this kind of useful function ever be secure?**
    - Response from DNP-UG: Unfortunately, time did not permit the panelists to respond to this during the session.
13. **Would you say that Zero Trust is the best approach to stop identity-based attacks that start from phishing and insider threat, lateral movement techniques, etc.? And how would that look like with the new upgrades to DNP3?**
    - Response from Grant Gilchrist: Zero-trust is a principle that would work against almost any attack, but as I understand it, it is being specified particularly because of attacks like Stuxnet and Ukraine, where software gets inside and is walking around for a while before anyone notices.
    - Response from Matthew Rogers: Zero Trust is about the journey, more than singular solutions (though SAv6 and AMP are great). I highly recommend our Maturity Model to help your organization think through that journey https://www.cisa.gov/zero-trust-maturity-model

- Comment from Ronald Farquharson: We have a white paper on how DNP3 security is addressing zero trust. Email me at r.farquharson@ieee.org for a copy.
- Follow-on question: Is that zero-trust white paper publicly available and referenceable?
- Response from Ronald Farquharson: As of right now the paper is being updated with new information. Please request it by email and we will send it to you when available.
- Further update from Ronald Farquharson: **This is the link** to our updated white paper on how DNP3 security is addressing zero trust.

14. **UL and SunSpec provide their own DER device certification programs. How DNP3 user group consider such certification programs?**
    - Response from Ronald Farquharson: Great question on certification! Yes, the DNP-UG has a Conformance Certification Program (CCP) that provides conformance certificates on successful completion. CCP services are discounted for most members. For more information reach out to us at admin@dnp.org.
    - Response from Grant Gilchrist: IEEE Std 1547 calls out DNP3 as one of the three protocols suites to be implemented for DERs. We are currently working on IEEE Std P1815.2 that shows what that mapping will look like. I would expect that eventually compliance with 1815.2 could be addressed by UL the way it has addressed the core 1547 spec.
    - Comment from DNP-UG: The UL / MESA DER certification verifies the DER functions of the devices but does not verify the DNP3 communication implementation. The DNP-UG provides Conformance Certification services for the DNP3 (IEEE 1815) communication protocol. Full certification of IEEE 1815.2 for DERs requires certification by both the MESA and DNP-UG certification programs.
    - Comment from Ronald Farquharson: 1547.3 is the guide for cybersecurity for DER communications. DNP3 SAv5 and SAv6 are indicated.
    - Comment from Frances Cleveland: Indeed, IEEE 1547 revision is looking to include some of the cybersecurity recommendations in IEEE 1547.3 and turn them into cybersecurity requirements if DERs want to interconnect to the grid
15. **What could be a good definition of IT and OT convergence?**
    - Response from Frances Cleveland: IT and OT are similar but different: Technologies in the Operational Environment (OT) have many differing security constraints and requirements from Informational Technologies (IT) environments. For IT environments, confidentiality of sensitive business and customer information is usually the most important. However, for OT

environments, the availability, authentication, authorization, and data integrity of power system information are usually the more critical requirements, since power data is typically not sensitive.

- Response from Grant Gilchrist: Regarding convergence, I think if the OT network is making use of the corporate PKI and actually using those credentials to authenticate and authorize field devices, that would make a lot of IT people sigh in relief. I think a key piece will also be intrusion detection systems that are customized to recognize the semantics of OT protocols. I heard a few years ago, for instance, that there are SNORT profiles available for DNP3.
- Response from Virginia Wright: CIE Implementation Guide: https://www.osti.gov/biblio/1995796

16. How DNP3 user group facilitates real-time threat intelligence sharing?

- Response from DNP-UG: Unfortunately, time did not permit the panelists to respond to this during the session.
- Response from DNP-UG: The DNP-UG does not have a mandate or mechanism for real-time threat intelligence sharing. It has published several Security Bulletins providing security-related information applicable to DNP3. Depending on the content, some of these are publicly available and some are restricted to the Member's Library.
- Response from DNP-UG: There are several organizations that facilitate threat intelligence sharing. For example:
    - The NERC operated Electricity Information Sharing and Analysis Center - E-ISAC - About the E-ISAC
    - Cybersecurity Risk Information Sharing Program (CRISP) which is a public-private partnership between the E-ISAC and the U.S. Department of Energy (DOE). CRISP
    - Energy Analytic Security Exchange (EASE) - Energy Analytic Security Exchange (EASE) – ISAO Standards Organization

17. Request: Could we have a session on IEC 61850 protocol security in future pls?

- Response from DNP-UG: Thank you for your suggestion. While many of our experts our also conversant with IEC 61850 protocol security, the focus of this group is IEEE 1815 (DNP3). For more information you may want to contact the UCA International Users Group at Home - UCAIug

- Response from DNP-UG: On a somewhat related note, several of our Cybersecurity Task Force members contributed significantly to the latest version of IEC 62351 Part 5 which has historically been closely aligned with DNP3 SAv5 and now with DNP3 SAv6.

Workshop Reference Information

1. The DNP-UG updated paper on addressing Zero Trust is **available here.**
2. CISA Secure By Design document for more details on shifting the burden of security to the design of products, provided by Matthew Rogers: https://www.cisa.gov/securebydesign
3. DOE CESER Cyber Informed Engineering website, provided by Virginia Wright: https://www.energy.gov/ceser/cyber-informed-engineering
4. NIST Cybersecurity Framework, mentioned by Frances Cleveland: https://www.nist.gov/cyberframework
5. Related, added by Mathew Rogers: NIST 800-82 is a good resource for talking through cybersecurity challenges from applying the Cybersecurity Framework to OT: https://csrc.nist.gov/pubs/sp/800/82/r3/final
6. Guidelines for Smart Grid Cybersecurity, mentioned by Grant Gilchrist: NIST IR 7628 Rev. 1 Guidelines for Smart Grid Cybersecurity (IR means “Interagency Report”): https://csrc.nist.gov/pubs/ir/7628/r1/final
7. The following resources on Cyber-Informed Engineering were kindly provided by Virginia Wright:
   a. Websites:
      i. DOE CESER CIE Website -- https://www.energy.gov/ceser/cyber-informed-engineering
      ii. INL CIE Website - https://inl.gov/cie/
      iii. NREL CIE Website - https://www.nrel.gov/security-resilience/cyber-informed-engineering.html
   b. Publications and Tools:
      i. CIE Implementation Guide: https://www.osti.gov/biblio/1995796
      ii. CIE Workbook for ADMS: https://www.osti.gov/biblio/1986517
      iii. CIE Workbook for Microgrids: https://www.osti.gov/biblio/2315001
      iv. CIE Workbook for Substations: https://www.osti.gov/biblio/2448237
      v. CIE Workbook for Water Systems: https://www.osti.gov/biblio/2371031

vi. CIE Analysis Tool: https://github.com/inlguy/CIE/releases/tag/v12.2.4.0

vii. CIRRUS - Tool for leveraging CIE for consideration of OT in the Cloud - Cirrus: Cloud Feasibility Assessment Tool for Grid Professionals available from INL Software

viii. CIE Microgrid Tool - Tool for leveraging CIE in the design of microgrids - https://github.com/idaholab/CIEMAT/tree/main

ix. Targeted R&D Guidance for CIE Principles

x. Web-based Implementation Guide

xi. CIE Quarterly Webinar: What is Cyber-Informed Engineering?

xii. CIE Study Case: Water Booster Pump Station - SLIDES

xiii. CIE Study Case: Water Booster Pump Station - WORKBOOK