Spotlight

Advancing Cybersecurity to Strengthen the Modern Grid

March 2019

Success Stories

U.S. DEPARTMENT OF ENERGY | Office of TECHNOLOGY TRANSITIONS

energy.gov/technologytransitions

Contents

Cybersecurity for Distributed Energy Resources

Sandia National Laboratories in conjunction with the Department of Energy Solar Energy Technologies Office, SunSpec Alliance, Electric Power Research Institute, National Renewable Energy Laboratory, and industry participants

Creating cyber security standards and best practices for interoperable distributed energy resources

Innovation

Distributed Energy Resources (DER) – energy generation and storage technologies that provide electricity which can include fuel cells, energy storage, solar, and wind systems – are being adopted by both utilities and the public. These systems require proven industry regulations to ensure security and attack-resilient structures to protect against future cyber threats. The US Department of Energy's Solar Energy Technologies Office asked Sandia to create a roadmap to improve cyber security for solar DER; the roadmap includes needs for cyber security research and development, standards development, and industry best practices.[1] As part of that efforts, Sandia, in conjunction with the SunSpec Alliance and partners, is conducting a DER cyber security workgroup to create standards in cyber security for DER.

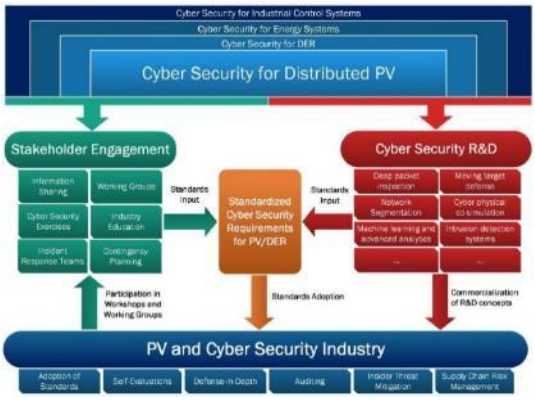
Outcomes

Technology Advancement

The SunSpec Alliance DER Cyber Security Workgroup is actively defining standardized certification procedures for DER and server vulnerability assessments; creating DER control network topology requirements and interface rules; and defining DER boundaries and requirements for transmitting data. Future projects will include classifying data types and permissions; defining protection mechanisms; establishing requirements for patching DER equipment; and creating recommended auditing practices for DER networks.[2]

Impact

The roadmap and the SunSpec Alliance Cyber Security Workgroup are creating a path for improving cyber security for DER systems, including communication-enabled PV systems, in which there are clear roles and responsibilities for government, standards development organizations, vendors, and grid operators.



Process for achieving cyber security of PV systems.
[Image: Sandia, Roadmap for Photovoltaic Cyber Security][1]

"Interoperable Distributed Energy Resources are rapidly becoming a large portion of the nation's power generation portfolio. These devices have the ability to provide grid services but also pose a risk to critical infrastructure if not properly secured. We established the DER Cybersecurty Workgroup to provide guidance, best practices, and cybersecurity standards for secure DER communications and control."
Jay Johnson, Principal Member of Technical Staff, Sandia National Laboratories [1]

Timeline

2017: Sandia and SunSpec Alliance launched the DER Cyber Security Workgroup

2017: Roadmap for Photovoltaic Cyber Security released

2018: US DER Interconnection Standard, IEEE 1547, is updated to require DER communications

[1] J. Johnson, "Roadmap for Photovoltaic Cyber Security," Sandia Technical Report, SAND2017-13262, Dec 2017.

[2] sunspec.org/wp-content/uploads/2018/10/5.SandiaDERCyber security-Gridvolution-9-12-2018.pdf

Cybersecurity for Energy Delivery Systems

Sandia National Laboratories in partnership with Lawrence Livermore National Laboratories, Washington Gas Energy Systems, Fort Belvoir, Chevron, Grimm, and Schweitzer Engineering Laboratories

Ensuring resiliency in energy and utility infrastructure through unpredictability and enhanced situational awareness in energy delivery system networks

Innovation

As critical infrastructure networks and control systems are upgraded and increasingly connected, system security is increasingly at risk. Energy delivery control systems traditionally have predictable communication paths and static configurations. Sandia's Artificial Diversity and Defense Security (ADDSec) project is developing solutions to introduce unpredictability and enhance situational awareness for vulnerable static energy delivery control systems, protecting them against cyber attack.

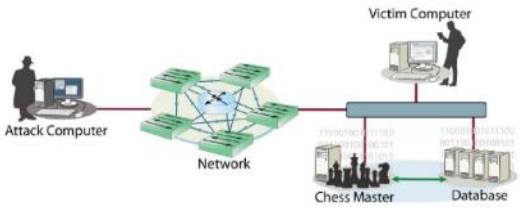
Outcomes

Technology Advancement

The ADDSec program has leveraged software defined networking to introduce random unpredictability into control system networks through three main components: network randomization, application library randomization, and machine learning based dynamic defense. Machine learning dynamic defense detects active attacks by recognizing patterns, providing situational awareness, and taking appropriate action when necessary.[1]

Impact

Research has resulted in a verified means for a resilient mechanism to support modern grid operation through creating complexity for adversarial attackers and detection capabilities for those attacks. Sandia, in conjunction with partner Schweitzer Engineering Laboratories, successfully employed testing at Fort Belvoir for ADDSec in which the technology defended Fort Belvoir's microgrid control system, detected abnormal behavior, and triggered a mitigation response. The demonstration has proven that the ADDSec technology can interoperate with commercially available products and be retrofitted into operating systems.[3]



Process demonstrating the security of legacy and modern systems by improving overall situational awareness and converting static systems into moving targets
[Image: Vicente Garcia. SNL][2]

"The detection and response capability of ADDSec provides a framework for Utility operators to proactively defend their networks against active threats in an automated fashion."

Adrian Chavez, Principal Member of Technical Staff / ADDSec Principal Investigator, Sandia National Laboratories[1]

Timeline[2]

October 2015: Project commences

July 2016: Initial Ft. Belvoir microgrid scenario developed

October 2016: Completed proof-of-concept demonstration

July 2018: Demonstration at Ft Belvoir microgrid for ADDSec certification

[1] DOE: energy.gov/sites/prod/files/2016/09/f33/SNL%20ADD%20Sec%20Fact%20Sheet%20September%202016.pdf

[2] SNL: energy.gov/sites/prod/files/2017/02/f34/SNL_ADDSec_Peer_Review_2016.pdf

[3] SNL. energy.sandia.gov/energy/ssrei/gridmod/grid-mod-newsletter/

Cybersecurity for Virtual Power Plants and DER Management Networks

Sandia National Laboratories

Creating secure control networks for distributed energy resources

Innovation

Virtual Power Plants (VPPs) and other distributed energy resource management systems (DERMS) require secure communications to decentralized power-generating units for reliable grid operations. Sandia National Laboratories is researching cyber security solutions for distributed energy resource (DER) control networks which provide these services while maximizing the security of the power system.

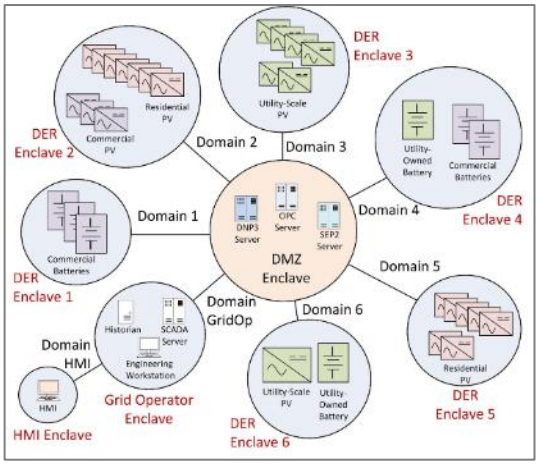
Outcomes

Technology Advancement

Sandia National Laboratories designed multiple network architectures to maximize security for grid services, and then evaluated these architectures using an adversary-based assessment methodology. SCEPTRE – a virtual power system and network platform developed at Sandia – is used to conduct red team assessments of these solutions in an isolated, safe environment where the team can study and quantify the tradeoffs between power system performance and cyber resilience.[2]

Impact

To date, Sandia has determined communication requirements for distribution and transmission grid services and deployed SCEPTRE to evaluate cyber resiliency. Three possible approaches to securing DER networks, i.e., enclaving, encryption, and moving target defense, have been assessed using red team methodology to advise the solar industry on the best cyber security practices.



Enclaved security reference architecture
[Image: Sandia National Laboratories]

"There are currently a lot of open questions in the DER industry about how to securely design communication networks. Sandia's secure architectures and red team assessments are laying the technical foundation for a secure smart grid of the future."

Jay Johnson, Principal Member of Technical Staff, Sandia National Laboratories

Timeline

2017: Completed 3-year Secure Virtual Power Plant Research Project

2017: Developed cyber security reference architecture

2018: Compared control/communications complexity for different approaches

[1] DOE. energy.gov/eere/solar/sunshot-national-laboratory-multiyear-partnership-sunlamp-photovoltaic-subprogram-fy16-18

[2] DOE. energy.gov/sites/prod/files/2018/09/f55/security_resilience_posters.pdf

Exe-Guard Whitelist Malware Protection Solution

DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and Sandia National Labs in partnership with Schweitzer Engineering Laboratories (SEL) and Dominion Virginia Power

A whitelist malware protection solution called exe-Guard protects the integrity of embedded devices in U.S. power control systems while minimizing the need for updating, security patching, and decommissioning.

Innovation

Instead of blocking device access to an ever-growing list of blacklisted malware, the exe-Guard system approves or whitelists a limited set of trusted programs or code. Using digital signatures and hash functions, this approach affords critical infrastructure protection (CIP) for control systems and lowers costs for administrative and operational management.[1]

Outcomes

Technology Advancement

Whitelist antivirus methods establish a security baseline and deny any code that deviates from that baseline state. The introduction of whitelist protection is particularly important for power systems, which rely on an embedded control system and monitoring devices that are difficult to access remotely.

While blacklist systems require frequent patches and signature updates to remain effective in stopping constantly emerging malware attacks, whitelisting allows less frequent security patching so that system decommissioning can be scheduled and planned.[1]

Impact

SEL was able to expand the original scope of this project and incorporate the exe-Guard technology into six separate products instead of the single product originally planned. This exe-Guard technology advanced the state of technology and is actively protecting America's power systems today.[1]

The SEL-3610 Port Server is one of multiple products embedded with exe-GUARD antivirus technology.
[Copyright: Schweitzer Engineering Laboratories][2]

"The exe-GUARD project has provided SNL with the unique opportunity of technically contributing to a commercial product that improves the security of energy delivery systems, that addresses CIP compliance standards, and that meets the operational needs of a major energy provider."[3]

Adrian Chavez,
Cybersecurity Scientist, SNL

Timeline[3]

December 2010: Exe-Guard project starts

November 2013: Commercial product development completed and field verification started

January 2016: Technology used in at least six commercial products from Schweitzer Engineering Laboratories. The products are widely deployed and now protect thousands of devices used in power control systems nationwide.[3]

[1] OSTI, Exe-Guard Project: Final Technical Report, Jan. 30, 2016. osti.gov/servlets/purl/1254473

[2] Image. selinc.com/products/3622/

[2] Quote. cdn.selinc.com/assets/Literature/Media/News/SEL_Embedded_exe-GUARD_Anti-Malware.pdf?v=20150812-080416

Interoperable Communication for Control Systems

Sandia National Laboratories and CESER in partnership with EnerNex Corporation, Schweitzer Engineering Laboratories (SEL), and Tennessee Valley Authority

Producing an open and interoperable security solution for utility control systems through metrics, network security tools, and testing.

Innovation

Among the major issues facing network security for critical infrastructure systems is interoperability for systems from different vendors. When purchasing network security products, control systems users have difficulty comparing products from different vendors due to the lack of an industry-wide mechanism to evaluate functionality, performance, and interoperability. Lemnos creates a universal way to describe and evaluate numerous control system security functions through identifying basic cybersecurity functions needed within industrial control systems, selecting solutions, and producing interoperable configuration profiles through comprehensive testing for cyber security functions.[2]

Outcomes

Technology Advancement

Sandia created an interoperable security architecture for common process control system add-on security devices and developed a reference implementation using open-source software and standardized hardware. In conjunction with SEL, Sandia transitioned the reference implementation to a commercial product using open-source software and connected the devices amongst nine other vendors to demonstrate security interoperability. Sandia provided technical expertise, prototype architecture, and design input.[3]

Impact

Lemnos provides a method to demonstrate interoperability through independently manufactured security product prototypes and has made it possible for vendors to develop interoperable solutions and create more reliable, clearly defined, and interoperable security devices by following an agreed-upon set of vocabulary and metrics.[4] The interoperable devices created by SEL and other vendors are now in use nationwide.

Schweitzer Engineering Laboratories' SEL-3620 Ethernet Security Gateway was developed as part of the Lemnos project.
[Copyright: Schweitzer Engineering Laboratories][2]

"This serves not only as the basis for secure field device critical infrastructure, but also serves as a shining example of the value that standards based interoperability can bring to the industry in general."

Erich Gunther, EnerNex Chairman and Chief Technology Officer[1]

Timeline

2006: Open Process Control Systems Security Architecture for Interoperable Design (OPSAID) program commences at Sandia in which SEL's security gateway is created

2009: SEL -3620 Ethernet Security Gateway created by SEL

2010: Lemnos program begins

[1] securitytoday.com/articles/2011/05/26/cybersecurity-interoperability-project-reaches-milestone.aspx
[2] researchgate.net/publication/291305786_Cyber_security_interoperability__The_Lemnos_project
[3] energy.gov/sites/prod/files/oeprod/DocumentsandMedia/5-Lemnos.pdf
[4] energy.sandia.gov/wp-content/gallery/uploads/OPSAID-Lemnos-Final-SAND-2012-0557Pno-marks.pdf
[6] selinc.com/products/3620/

Legacy Communication Monitoring (SerialTap™)

DHS Science and Technology Directorate (DHS-ST) and Pacific Northwest National Lab in partnership with Cynash Inc.

SerialTap™ brings a new layer of security to older industrial control systems. As its name suggests, this patented sensor passively taps directly into serial communication systems, monitoring network traffic and watching for control signal anomalies that could indicate a cyberattack.

Innovation

SerialTap™ is a low-cost, compact, embedded device for passively tapping serial line communication and transmitting it over an Ethernet network for comprehensive control system situational awareness. Cost-effective and nonintrusive, SerialTap™ integrates easily with common IT enterprise security solutions.[1]

Outcomes

Technology Advancement

SerialTap™ connects legacy technologies to a computer network and commercial advanced cybersecurity software to monitor older systems. Without interrupting system operations, it "translates" the data from the control system for network cybersecurity software analysis, allowing the identification of anomalies like cyberattacks, speeding their resolution and potentially saving millions of dollars in downtime.[2]

Impact

Large portions of industrial control systems continue to be operated with legacy serial communications, and have largely been ignored by the cybersecurity community. This has led to one of the biggest challenges for ICS operators—retrofitting cybersecurity solutions to legacy systems. The ability to monitor traffic in these environments is necessary to provide complete situational awareness of ICS security states.

The Cynash SerialTap™ brings a new layer of security to older industrial control systems.
[Image: Cynash Inc.][3]

"SerialTap enables us to get safe and secure visibility into serial communications in industrial control environments. This has given us access to data that was not previously attainable and has led to new opportunities for development in behavioral and predictive modeling, as well as enhanced cyber protection capabilities."

Jessica Ohnona
Director Data Science, Intelligence and Analytics
Cynash Inc.

Timeline

2010: PNNL develops initial prototype

2013 - 2015: SerialTap™ technology matured and promoted through DHS Transition to Practice (TTP) program

2017: Cynash Inc. commercially releases SerialTap™ technology

[1] TTP Technology Guide. dhs.gov/sites/default/files/publications/CSD_TTP_Guide_2018_webversion_06262018_508%20Final.pdf
[2] R&D 100 Award Winner rd100conference.com/awards/winners-finalists /6722/serialtap/
[3] Image and Quote. cynash.com/#our-technology

Link Module with Secure SCADA Communications Protocol (Hallmark)

Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and Pacific Northwest National Lab in partnership with Schweitzer Engineering Laboratories (SEL) and CenterPoint Energy Houston Electric

A Secure SCADA Communications Protocol (SSCP) uses authentication and optional encryption to protect communications between remote devices and central control centers.

Innovation

This technology ensures that all SCADA systems' device-to-device communication comes from an authorized and trusted source. Works with both existing and new devices by sending messages between devices with a device identifier. Can also encrypt the data to provide more security to the grid.

Outcomes

Technology Advancement

SEL designed a serial shield (SEL-3025) that plugs into serial communication link between a legacy device and the system. This device adds a small amount of latency while secure serial communications with SSCP. Another device produced from this project, the SEL-3045, is a cryptographic card that is a hardware card that runs the SCCP within a device.

Impact

The devices developed as part of the Hallmark project will be able to establish secure SCADA connections for both new and legacy devices. In addition, these systems incorporate easily into the new system designs. Encryption of SCADA data secures the serial communications between devices.

SEL-3025 Serial Shield device. Is placed next to equipment that transmits data so the signal can be encrypted.
[Copyright: Schweitzer Engineering Laboratories][2]

"Encryption provides confidentiality and integrity for remote monitoring and interactive remote access and locks out malicious intruders from your critical assets. With its remote management functionality and wide range of application support, the SEL-3025 is flexible and easy to use."
SEL-3025 Product Brochure

Timeline[3]

October 2007: Start of Project Period

June 2010: Link module and cryptographic card released

March 2012: End of Project Period

[1] Image: selinc.com/products/3025/

[2] SEL Brochure: cdn.selinc.com/assets/Literature/Product%20Literature/Flyers/3025_PF00246.pdf?v=20180418-133153

[3] OSTI: osti.gov/servlets/purl/1087721

Micro-Synchrophasor Measurements to Secure Power Distribution Systems

Lawrence Berkeley National Laboratory and the Office of Cybersecurity, Energy Security, and Emergency Response in partnership with ARPA-E, Power Standards Lab, EnerNex, EPRI, Riverside Public Utilities, and Southern Company

Micro phasor measurement units (μPMUs) capture data about the state of the power grid and combine that data with supervisory control and data acquisition (SCADA) information to provide real-time data on system performance.[1]

Innovation

Allows utilities to detect a physical or cyber grid disruption using μPMUs. Synchophasors are able to provide data much faster than SCADA systems and are especially useful when installed at facilities such as substations. The collected data from μPMUs is combined and sent to SCADA systems to provide real-time feedback on the state of the grid. Abnormal behavior on the grid such as a cyberattack can therefore be detected by this system.

Outcomes

Technology Advancement

Increases the amount of data provided by field sensors by using μPMUs which take measurements 120 times per second, roughly four times more than current phasor measurement units (PMUs). In addition, μPMUs are smaller and less-expensive than traditional PMUs which allows more to be used and more data to be collected. The team at Berkeley also modified an existing machine-learning algorithm to detect abnormal behavior in the power grid by examining differences between SCADA and μPMU data.[2]

Impact

This technology increases grid reliability and resiliency by allowing for faster detection of a cyber or physical disruption of the grid. The increase in local devices and associated communications infrastructure is also an advance for Internet of Things (IoT) technologies. Future μPMU devices should secure distributed energy resources (DERs) such as rooftop solar panels and make it easier to incorporate higher penetrations of DERs.

A μPMU installation on a utility distribution pole. There is a GPS antenna on top of box and a high resolution power quality monitor.
[Image: ARPA-E][3]

"The idea is if we could leverage the physical behavior of components within the electrical grid, we could have better insight in terms of whether there was a cyberattack that sought to manipulate those components. These devices provide a redundant set of measurements that give us a high-fidelity way of tracking what is going on in the power distribution grid"[4]

Sean Peisert,
Computer Scientist and, LBNL

Timeline

2015: LBNL cybersecurity project starts

2018: LBNL project moves to tech transfer phase.

[1] Other. dst.lbl.gov/security/project/ceds-upmu/

[2] GCN. gcn.com/articles/2018/09/21/grid-cybersecurity.aspx?m=1

[3] Image. arpa-e.energy.gov/sites/default/files/documents/files/UCB_OPEN2012_ExternalProjectImpactSheet_FINAL.pdf

[4] Quote. cs.lbl.gov/news-media/news/2018/combination-of-old-and-new-yields-novel-power-grid-cybersecurity-tool/

Secure Information Exchange Gateway for Electric Grid Operations (SIEGate)

Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and Pacific Northwest National Lab in partnership with Grid Protection Alliance and others

An open source software tool that maintains the integrity of large data sets sent between transmission organizations and control centers.

Innovation

A secure and flexible program that serves improves the security of electrical utility control centers while minimizing their external exposure to cyber attacks. The system allows for SCADA data, synchrophasor data, alarms, and notifications to be exchanged at low latency. SIEGate strengthens cybersecurity and relieves administrative burdens and costs of data sharing between control centers.

Outcomes

Technology Advancement

SIEGate is capable of exchanging 5 million measurement data points per second among control centers and devices. The SIEGate project introduces an appliance that serves as a gateway to exchange multiple types of data required for real-time electric system operations. SIEGate allows legacy systems to send secure and reliable data to control centers. Making the software open source lowers the cost of the product and makes it widely accessible.

Impact

This software will improve security for control centers by replacing the need for a multitude of devices to exchange power system data and introducing a single, secure gateway appliance. SIEGate also reduces management and overhead costs associated with more complex systems.

Logo for SIEGate open source software. The code is open source and available on GitHub.
[Grid Protection Alliance][1]

"SIEGate is capable of moving a large and continuously varying set of data at low latency… A single instance of SIEGate on common hardware can exchange about 5 million measurements points per second"
Grid Protection Alliance Product Page [1]

Timeline[2]

2010: Work begins on SIEGate

2013: Initial version published

2017: Program has been download more than 3,000 times

[1] Image: gridprotectionalliance.org/products.asp
[2] GitHub: github.com/GridProtectionAlliance/SIEGate