Transforming Cybersecurity

How PNNL automates cyber defense and resiliency

Pacific Northwest NATIONAL LABORATORY

Protecting critical infrastructure from cyber threats requires new approaches to proactive, machine-speed defense. Through a portfolio of unclassified research and classified applications, PNNL brings scientific and engineering rigor to disrupting and deterring cyber adversaries. PNNL develops next-generation capabilities for cyber analytics and situational awareness, resilient system design, assured automation for cyber systems, consequence prediction of cyber effects, and real-time dynamic response. Together, these advances give the United States a strategic advantage against rapidly evolving adversary capabilities.

A MODERNIZATION AGENDA FOR RESILIENT, MACHINE-SPEED SECURITY

To counter growth in our adversaries' sophistication, PNNL harnesses the integrated power of advanced computing, data analytics, and artificial intelligence and machine learning (AI/ML) to invent a new generation of trusted cyber automation. PNNL's deep expertise in **AI and human-machine teaming** provides the science foundation to accelerate the discovery of complex threat indicators in energy systems and create **autonomous resilience**—systems that predict and mitigate consequences of failure across linked cyber and physical domains. Introducing AI into critical infrastructures requires a new level of **trust and assurance of AI systems**; PNNL's AI security agenda reduces the vulnerability of AI to adversarial attack and increases confidence in AI processes. PNNL also advances the **security and integrity of 5G networks** while bringing new analytics to the energy system edge and the internet of things (IoT), thereby increasing efficiency and robustness of future energy systems and their communications networks.

PNNL's vision to move converged IT and operational technology (OT) networks from rear-view analysis of cyber intrusions to **forward-looking, proactive, and real-time discovery of and response to adversary activities** supports the Administration's priorities for IT modernization and shared cybersecurity services. In particular, the SURGEPROTECTOR effort connects multiple offices across DOE to invent transformative sensing, analytics, and decision support for converged IT and OT systems, thereby establishing a new level of trusted security automation.

ADVANCING CYBERSECURITY FOR THE DOE ENTERPRISE

PNNL plays a leading role in cyber defense for the DOE enterprise through the Cooperative Protection Program (CPP), which provides cyber situational awareness for 90% of the DOE Complex and has provided critical insight into recent attacks on DOE networks. Complementing CPP, the Cyber Intelligence Center (CIC) performs classified analysis of adversary information-seeking activity on DOE networks. PNNL also draws on the results of its extensive cybersecurity research portfolio for DHS, DOD, and other agencies to bring new capabilities to DOE. This includes establishing the mathematical and computer science foundations to move **beyond signature-based detection methods** that rely heavily on humans in the loop **to machine-speed reasoning**, create improved situational awareness of the cyber battlefield, and invent **automation that supports proactive maneuvering** around attacks and faults.

To validate the efficacy, trust, and security of these advanced cyber capabilities, PNNL has implemented a Living Laboratory model, enabling cybersecurity researchers and operators to

partner in piloting cybersecurity solutions at PNNL first, as well as using PNNL's deep cyber operational expertise to inspire the next generation of cybersecurity technologies.

TRANSFORMING CYBERSECURITY TECHNOLOGY FOR ENERGY SYSTEMS

PNNL's cybersecurity expertise is driving the convergence of information technology (IT), industrial controls systems (ICSs), the IoT, and advanced communications systems such as 5G in support of DOE's capability base for energy sector security.

Building on the information-sharing advances of CPP and the intelligence analysis strengths of CIC, PNNL leads the Cybersecurity Risk Information Sharing Program (CRISP) with the North American Electric Reliability Corporation (NERC) Electricity Information Sharing and Analysis Center (E-ISAC). CRISP is a voluntary information-sharing and threat intelligence program for the energy sector that **covers more than 75% of U.S. electricity customers** and is expanding to the oil and natural gas sector. PNNL's novel analytics integrate cybersecurity data from utilities with classified threat reporting to create a holistic and timely picture of threat conditions that inform the defensive actions of participating utilities.

Using its expertise in advancing the mathematical and computational foundations of risk modeling, PNNL works with DOE's Office of Electricity on the North American Energy Resilience Model (NAERM) effort to **improve defense of power system assets** and with DOE's CESER and other agencies to increase **supply chain security** for energy systems. PNNL is advancing risk reduction beyond basic assessment methodologies to science-based dynamic optimization that reduces adversary effectiveness.

Through its agency-wide R&D support to the DHS Cybersecurity and Infrastructure Security Agency (CISA), PNNL is creating techniques for ICS security scanning and vulnerability discovery, crafting new ML methods for automated threat hunting, and centralizing and orchestrating service restoration for the civilian government after a major cyber event. PNNL also uses its deep expertise in energy system security to understand vulnerabilities in adversary infrastructure in support of partner agency missions.

PNNL is recognized for **implementing innovative programs to rapidly scale the talent base** in areas of critical expertise for the nation. Through efforts such as the Public Infrastructure Security Cyber Education System (PISCES), technical bootcamps and executive-level courses, and innovative virtual and augmented reality training environments, PNNL plays a leading role in upskilling practitioners and bringing new talent into the cybersecurity community.

ABOUT PNNL

Pacific Northwest National Laboratory advances the frontiers of knowledge, taking on some of the world's greatest science and technology challenges. Distinctive strengths in chemistry, Earth sciences, biology, and data science are central to our scientific discovery mission. PNNL's research lays a foundation for innovations that advance sustainable energy through decarbonization and energy storage and enhance national security through nuclear materials and threat analyses.

CONTACT

Deb Gracio, Associate Laboratory Director, National Security
(509) 375-6362 | Debbie.Gracio@pnnl.gov | www.pnnl.gov/cybersecurity,
http://www.pnnl.gov/artificial-intelligence

February 2021
PNNL-SA-159619

Pacific Northwest
NATIONAL LABORATORY