



Securing the Nation's Critical Infrastructure

Cybersecurity

OUR NATION'S CHALLENGE

The cyber-attacker of today has an advantage over those protecting our Nation's assets and infrastructure – they can operate inexpensively, with anonymity, and without pressure to act quickly.

At the Pacific Northwest National Laboratory, we understand the enormity of this challenge and the need for rapid threat discovery utilizing both traditional and non-signature based cyber solutions.

PNNL'S APPROACH

Since the late 1990s, PNNL has provided impactful cybersecurity research and solutions to protect our Nation's cyber infrastructure. Today, PNNL staffs over 300 hundred scientists and engineers, who are engaged in multi-disciplinary teams that include not only cyber professionals, but also biological, chemical, high performance computing, and software engineering expertise. Our resources and expertise are deployed in solutions for the U.S. Departments of Energy, Homeland Security, Defense and other National Security agencies.

Additionally, PNNL remains committed to significant multi-year cybersecurity research investments. Our current agenda is intended to produce the tools and technology that will not only measure the cybersecurity posture at all system levels, but provide an asymmetric advantage to the defender at reduced operational costs.

How do we know if we are on track? The evaluation, analysis, and visualization of these grand challenges and other transformational ideas happen every day at PNNL's Cyber Innovation and Operations Center—a secure prototyping and demonstration capability where we advance the analytic state-of-the-art and address emerging customer needs.

Our extensive portfolio of technology and capabilities offers tomorrow's innovative solutions today; each designed to enhance the nation's cyber-security posture in the areas of:

- » Global Threat Intelligence
- » Electric Grid Security
- » Cyber Physical Systems
- » Bio-inspired Security
- » Component Security
- » Cyber Analytics

CONTACTS

For more information about Cybersecurity solutions and capabilities, contact:

Troy Thompson — Cybersecurity Account Manager
Troy.Thompson@pnnl.gov

Mike Bettinson — Secure Cyber Systems Technical Group Manager
Mike.Bettinson@pnnl.gov



DISCOVERY

in action

Global Threat Intelligence

PNNL researchers and engineers have designed, deployed, and operate a cyber-defensive system that collects, characterizes, and enables the analysis of network traffic for Department of Energy facilities located throughout the United States. This unique capability, coupled with PNNL's expertise, receives national recognition for its ability to track, analyze, and scope cyber threats across the DOE complex.

Cyber Physical Systems

Research at PNNL examines vulnerabilities associated with cyber-physical interdependencies. Using existing facility information regarding layout, network topology, and installed safeguards, our researchers evaluate a facility's ability to detect, delay, and respond to attacks. By identifying vulnerabilities and evaluating safeguards, we can provide a better defense against threats or adversaries.

Electric Grid Security

PNNL is leading the charge to secure a safer and more reliable grid. We are currently developing cyber-based systems that safeguard our Nation's critical electric infrastructure in projects such as the Pacific Northwest Smart Grid Demo Project. Additionally, PNNL's ability to fuse data between simulated and physical equipment utilizing virtualization enables the creation of realistic and scalable environments where new functionality and ideas can be exercised.

Bio-inspired Security

Cited as one of the 10 most innovative ideas in Scientific American, the DigitalAnts™ solution developed by PNNL reduces the level of human involvement required in problem detection and resolution while retaining the human ability to intervene as desired. Another approach models computational data as if it were a human gene sequence, enabling a moving target defense mechanism for identifying cyber entities.

Component Security

Computer scientists at PNNL began research involving component security over a decade ago. Today these unique tools are helping United States government agencies assure the integrity of their mission-critical systems. For example, ensuring the integrity of computer hardware and firmware components; developing specialized diagnostic and monitoring tools; identifying malicious code that is undetectable by operating system tools and the detection of pirated hardware and compromises in the supply chain of mission-critical systems.

Cyber Analytics

Our innovative and distinctive methods, algorithms, and software tools, combined with large scale data management and available data tools enable PNNL domain experts to detect anomalies and defend computer networks. These analytic capabilities are used in applications from enterprise-level situational-awareness to individual host anomaly detection.



Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** Since 1965