Pacific Northwest
NATIONAL LABORATORY

The palm-sized SerialTap developed at Pacific Northwest National Laboratory (PNNL) protects legacy industrial control systems by connecting to serial communication devices to provide much-needed situational awareness for detecting potential cyberthreats.

SERIALTAP CYBERSECURITY TOOL

Enabling complete situational awareness in control systems

A FIRST-OF-ITS-KIND SOFTWARE TOOL

Most cybersecurity tools and methods are highly sophisticated, designed to protect critical data from attackers around the globe. But some older industrial control systems, such as those that manage the operation of transportation systems and the delivery of water and electricity, cannot interact with today's cybersecurity tools. The systems number in the millions and may be vulnerable to cyberthreats. When communications lines to these remote operations or serial devices are connected to the IT networks of industrial control systems, it may leave them open to bogus commands that could do serious damage.

Researchers at PNNL have developed SerialTap, a first-of-its-kind technology that bridges the gap between older, serial-based devices and modern networks in industrial control systems.

SerialTap taps into these older communications devices to translate information and mitigate threats. The award-winning technology is an inexpensive means of wrapping the data from the serial communications device in a form that can be used by modern assessment tools that don't "speak the same language," thus providing situational awareness to a company's engineering and security team.

TECHNOLOGY FEATURES

- Addresses vulnerabilities inherent in remotely controlled physical systems common in infrastructure and manufacturing.
- Bridges the gap between older, serial-based devices and modern networks.
- Provides data from many industrial control systems—sensors, switches, valves, relays, workstations, servers, and control computers—all in various field locations.
- Inexpensive and compact.
- No interruption to systems operations.
- Early detection of cyberattacks and network anomalies.
- Speeds resolutions; failsafe.

U.S. DEPARTMENT OF ENERGY

Researchers at PNNL create solutions to our nation's toughest challenges in energy resiliency and national security. Often, federally funded research results in intellectual property that is available for licensing. Visit our available technologies website to view this portfoilo.

pnnl.gov/available-technologies

SerialTap addresses vulnerabilities inherent in remotely controlled physical systems common in infrastructure and manufacturing.

CONNECTS LEGACY TECHNOLOGIES TO CYBERSECURITY

The palm-sized device is an inexpensive, nonintrusive add-on that can monitor and verify the activity in older serial communication systems. Without interrupting system operations, SerialTap "translates" the data from the control system so the network cybersecurity software can analyze it, allowing the detection of cyberattacks and network anomalies, speeding their resolution, and potentially saving millions of dollars in downtime.

SerialTap is a sensing device only. It passively monitors serial communications and transmits information to more advanced tools to analyze data. Used alone, the tool has no ability to prevent or hinder a cyberattack.

However, without a device like SerialTap, those charged with preventing or mitigating cyberattacks won't know an attack has happened until it has caused catastrophic or potentially irreparable harm. With the software tool, infrastructure owners can monitor the status of their legacy industrial control systems and act as soon as an anomaly arises.

Available for licensing, SerialTap is demoed here for use on a water tank.

GAIN SITUATIONAL AWARENESS

SerialTap offers many benefits over existing solutions, including the following:

- An inexpensive, compact, and elegant way to connect legacy technologies to a computer network and cybersecurity software to monitor older systems and gain situational awareness.
- No interruption to system operations, as SerialTap passively "translates" the data from the control system so the network cybersecurity software can analyze it.
- Early detection of cyberattacks and network anomalies, and it also helps speed their resolution, potentially saving millions of dollars in downtime.
- Can provide data from a variety of industrial control systems, such as sensors, switches, valves, relays, workstations, servers, and control computers, all in various field locations.
- Able to adapt automatically, allowing ability to be implemented across different networks without the need for customization.
- Designed to act in the background (passively), making it failsafe; any failure of the tap would not interrupt system operation.

INDUSTRY APPLICATIONS

SerialTap was developed through the Department of Homeland Security's Transition to Practice Program, which is designed to expose promising cyber technologies to entrepreneurs and potential investors.

The invention is available for licensing in all fields of use and is ideal for critical energy, transportation, oil and gas production, and industrial infrastructure systems that still rely on legacy control systems.

LET'S CONNECT

If you have questions, regarding this technology, please send inquiries to commercialization@pnnl.gov. You can view all PNNL technologies available for licensing at www.pnnl.gov/available-technologies.