Pacific Northwest
NATIONAL LABORATORY

Cyber Isolets – Ubiquitous Segmentation

The challenge/need

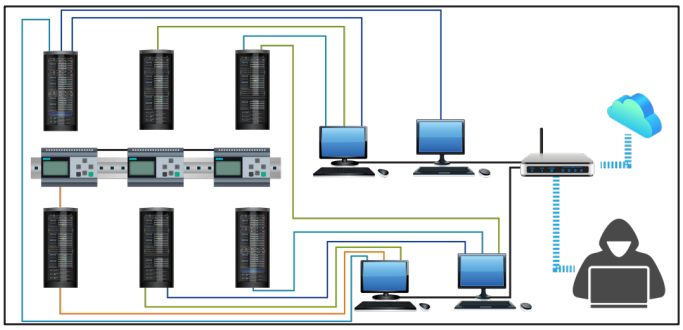
Industrial Control Systems and Supervisory Control and Data Acquisition systems are used to monitor and control equipment in a plant or in the field. They are common in industries such as energy utilities, telecommunications, water and waste control, transportation, and oil and gas refining. Industrial cybersecurity in the operational technology setting is challenging.

There is a bridge between these systems and other business-related networks due to the need to exchange data, information, and files. Many cyberattackers attempt to exploit this bridge between business and operational systems by jumping between applications or across networks.

APPROACH

Pacific Northwest National Laboratory has developed a new approach—called adaptive integrated isolation—to counter these sophisticated cyber threats without disrupting work flow through its Proactive Adaptive Cybersecurity for Control (PACiFiC) project.

PACiFiC combines adaptive principles, cross-domain information, and classic security best practices to deliver measurably more secure, reliable, robust, and resilient control systems while retaining business performance. By unifying disparate data and information from multiple domains, including human, cyber, communications, and process physics, PNNL has defined and established secure design principles for use in all operational technology systems across multiple critical infrastructures.



Cyber Isolets allows creation of segments around specific business processes or services within a host and across a network to isolate different levels of critical data and applications while still allowing users to perform their jobs effectively.

HOW IT WORKS

Patent-pending Cyber Isolets uses a zero-trust cyber architecture for ubiquitous segmentation with complete mediation of data exchange.

When physical isolation isn't practical, it is necessary to develop technical measures that provide robust and resilient security barriers to inhibit threats while minimizing impact on business processes.

Cyber Isolets provides the foundational new architecture design, based on secure system design principles, that creates isolated environments where only specific applications should be operating.

Existing cyber protections do not consider all the elements of access and operate independently of one another, leaving security gaps, which are exploited by adversaries to further compromise networks. Cyber Isolets takes adaptive, integrated

measures to isolate users, applications, and essential functions to achieve ubiquitous segmentation. Think of these separations as layered, concentric partitions that limit where users can get to within a system, based on multiple layers of applications.

Cyber Isolets maps users, applications, and network segments through a policy and design approach. Through an integration of cutting-edge techniques in application isolation and network segmentation, Cyber Isolets enables ideal least privilege and separation of privileges, and provides a foundation for adaptive, proactive, and active defenses.

BENEFIT

The user sees very little change in interface while maintaining an effective defense against sophisticated threat tactics that leverage business processes to pivot to operational technology systems like relays and circuits within critical infrastructure.

Cyber Isolets integrates operational security and network compartmentalization to thwart these “pivoting” threat tactics.

If an attacker sends a phishing email, for instance, it will open only in an area where there is limited availability, preventing connection with command and control infrastructure and movement to other operational applications. However, employees can still utilize web services to the internet and other internal systems along with their specialized applications, the same as they do today.

Cyber Isolets enables high-resolution segmentation of data based on business processes.

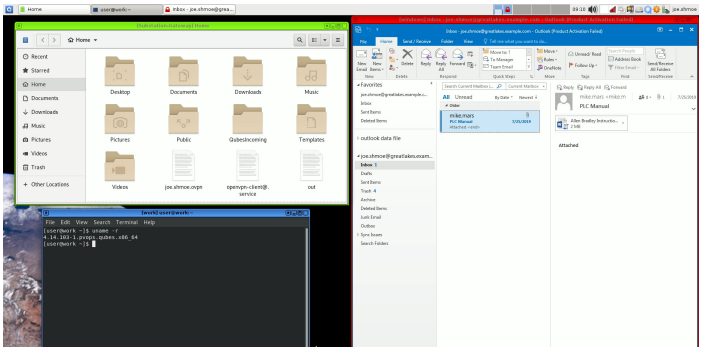
End-to-end segmentation provides new opportunities for sensing and analytics, which enable security orchestration automation response (SOAR)/moving target defense and integrated deception for “rat hole” defense.

Cyberattacks are derailed without disrupting organizational efficiency. In short, Cyber Isolets protects systems with less user disruption, making sure that businesses can run efficiently and securely.

IMPACT

Current threat tactics are thwarted by Cyber Isolets and critical systems are protected from intrusion and manipulation. The user sees very little change in interface while maintaining an effective defense for current attack behavior and threat tactics that leverage business processes to pivot to operational technology systems.

The Cyber Isolets technology achieves isolation of critical control center systems and applications while enabling data exchange with the business networks and enforcing security barriers.



The PNNL prototype of Cyber Isolets uses the Qubes OS to provide application isolation and specialized features that integrate with network segmentation technology. Each colored window represents a different cyber isolet in the host and across the network.

For more information, contact:

Tom Carroll
Cybersecurity Researcher
National Security Directorate/Computing & Analytics
Pacific Northwest National Laboratory
509.371.6731 | Thomas.Carroll@PNNL.Gov

Thomas Edgar
Cybersecurity Researcher
National Security Directorate/Computing & Analytics
Pacific Northwest National Laboratory
509.372.6195 | Thomas.Edgar@PNNL.Gov

www.pnnl.gov

PACiFiC

PNNL-SA-147970 | 10/1/2019

U.S. DEPARTMENT OF ENERGY