perspecta LABS

Jolt

Uncover sophisticated power grid attacks with intelligent telemetry defense

Key Jolt benefits

- Find inconsistencies in grid state telemetry via reported values from local and remote sensors and out-of-band sources
- Intelligently analyze and aggregate discrepancies to detect misreporting and configuration errors
- Combine grid telemetry with state-of-the-art power models to detect suspect devices and neutralize threats

Perspecta Labs' Jolt, part of its Secure**Smart™** critical infrastructure solution line, is a state-of-the-art power analyzer for substation telemetry defense. Jolt defends utility supervisory control and data acquisition (SCADA) and industrial control systems (ICS) from complex attacks that corrupt substation protection relays, automation controllers, remote terminal units (RTU) and energy controllers.

Jolt extracts grid state information from control center and substation telemetry and applies the constraints of a physical energy model to detect telemetry inconsistencies and fraudulent devices. Unlike a traditional intrusion detection system or Layer 4 inspection device, Jolt interprets the energy measurements in DNP3/IP, DNP3/Serial, IEC 61850 Generic Object Oriented Substation Events (GOOSE), relay metering, Secure**Smart** AMI/DA telemetry, and direct feeder sensors and reconciles the readings across multiple interconnected controllers and substations. Developed under a U.S. Department of Defense ICS cybersecurity project to defend the grid against Ukraine-like attacks, Jolt operates both at a substation level and a grid level, and provides advanced misbehaving controllers altered by code or data attacks for smart grid and other ICS and SCADA applications.

Advanced protection for evolving threats

Cyberattackers increasingly employ deceptive techniques to avoid detection. Attackers can use malware to penetrate the devices that monitor and manage the power grid and falsify the data they report or maliciously alter their configuration. Jolt can detect sophisticated protection and automation system compromises in individual and multi-substation environments.

Jolt applies smart analytics to validate real-time telemetry with circuit topology for rapid response and robust substation defense.

Jolt's thorough analysis combines data and information from grid topology devices, underlying operations technology (OT)

sensing and control devices, RTU, real-time automation controller (RTAC), energy management system and information technology communications devices. Jolt's sophisticated analytics can then enable fast identification of the root cause of cyber-based disruptions and rapid localization of suspect devices.

Jolt's innovative components and capabilities include:

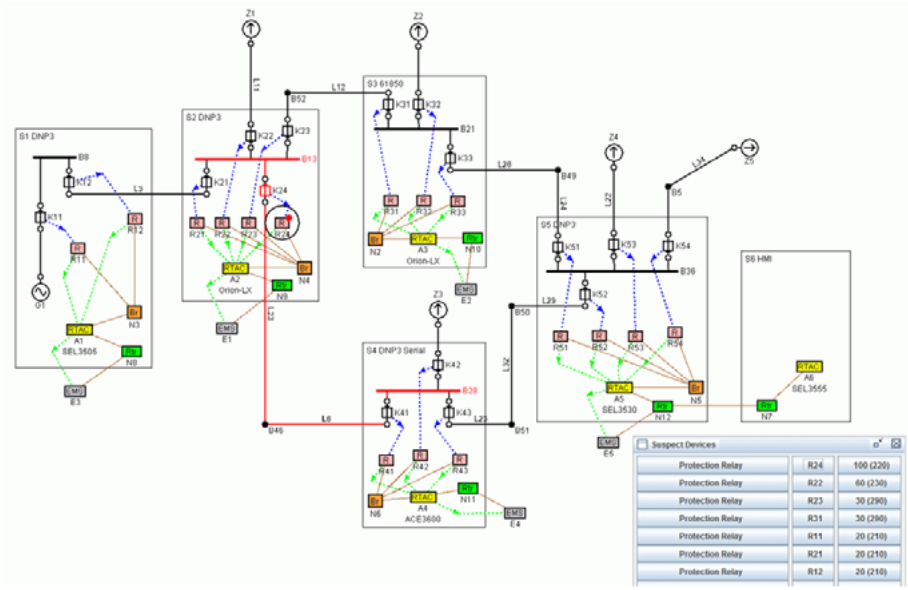
- A topology editor to construct one-line energy diagrams and SCADA reporting structure for measurement sources
- A state repository with standard data on measurement values and device states
- Power analytic algorithms to detect inconsistent states in the grid
- A probable cause analyzer to relate inconsistencies back to the infrastructure and to rank order suspicious OT devices
- A what-if capability to compare potential causes of grid disruption to expected values

Jolt analyzes grid state information from real-time telemetry intercepted from grid devices. Jolt supports DNP3 and IEC 61850 messages exchanged between devices and management systems. Jolt can work with multiple redundant sources of sensor data as well as human reporting. Jolt uses consistency checks on telemetry data to verify that devices are not corrupted. Devices are awarded "trustworthiness" scores based on the consistent and inconsistent analyses in which they participate.

Comparing Jolt to other tools

Cybersecurity tools employed in ICS and power system applications typically reside in a gateway and offer traditional capabilities such as firewalls, VPN, port scanning and intrusion detection applications. Jolt is the industry's first power analyzer for monitoring the integrity of substation telemetry. Jolt rapidly detects misreporting and configuration errors and identifies suspect devices by analyzing inconsistencies in grid state telemetry in complex cyberattacks.

Jolt detecting deceptive RTAC with out-of-band reporting



About Perspecta Labs

At Perspecta Labs, we refuse to think inside the box. As the innovation hub of Perspecta, we are molding the future of emerging technologies. Our experts conduct leading research into machine learning, artificial intelligence, mobile communications and internet of things technologies that provides customers with transformative insights and real-time situational intelligence. With our finger on the pulse of next-gen technology, you'll gain an essential edge.

Drawing on our Bell Labs and Applied Communication Sciences heritage, Perspecta Labs creates innovative technologies and services to solve the most difficult and complex information and communications challenges.

© 2019 Perspecta Labs

perspectalabs.com | info@perspectalabs.com
150 Mount Airy Road
Basking Ridge, NJ 07920