ENGINEERING

JOLT

Prevent Sophisticated Power Grid Attacks via Cyber Analysis of Power System Telemetry

ADVANCED DETECTION FOR EVOLVING THREATS

Cyberattacks increasingly employ deceptive techniques to avoid detection. Attackers use malware to penetrate the devices that monitor and protect the power grid to falsify reporting or maliciously alter their configuration.

Peraton Labs' Jolt is a real-time, state-of-the-art cybersecurity analysis tool for electric grid systems. A security application in the SecureSmart™ critical infrastructure solution line, Jolt employs a new method of detecting sophisticated compromises in protection and automation systems by analyzing supervisory control and data acquisition (SCADA) telemetry measurements. Jolt applies cybersecurity analytics to reason about real-time telemetry within the context of the circuit topology, independent of energy management systems.

HOW JOLT WORKS

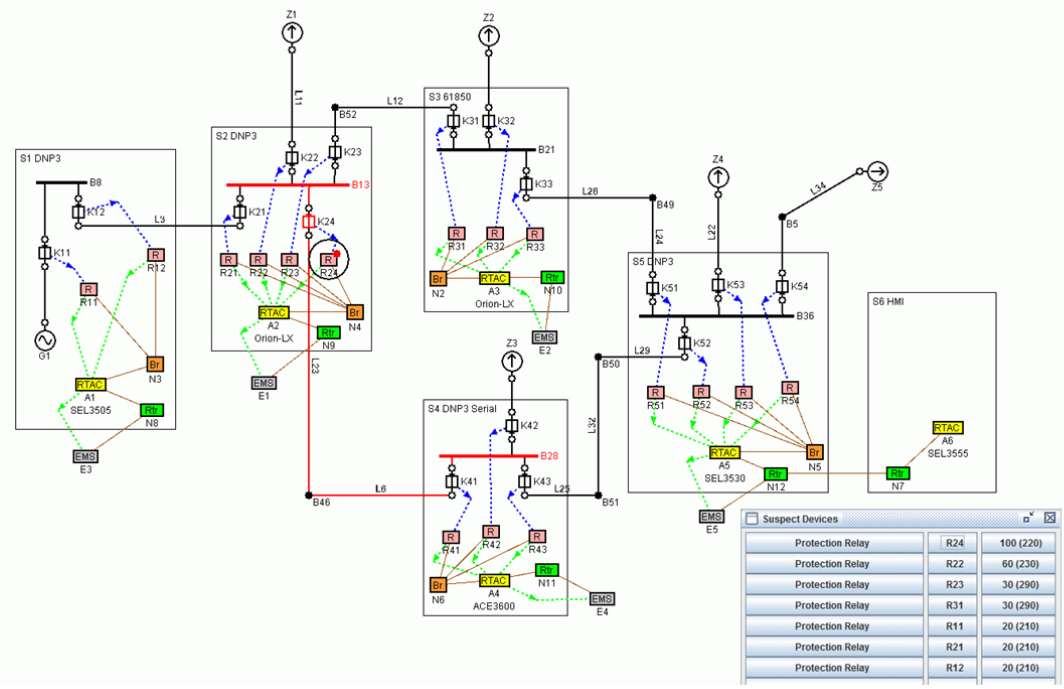
Jolt passively extracts grid state information from SCADA traffic and other sources. It corroborates measurements from multiple sources that either directly report on – or can be used to derive data on – common points within the grid. It then applies the constraints of a physical energy model to detect and reason about inconsistencies. Jolt rank orders a list of suspect devices, reports evidence of the inconsistencies, and identifies the highest ranked devices in the control system diagram for investigation.

Unlike traditional intrusion detection systems or Layer 4 inspection devices that look at transport protocol wrappers, Jolt interprets the application-level payload measurements exchanged in industrial control system (ICS) protocols with knowledge of system point maps. Jolt analyzes and reconciles the readings across multiple controllers and substations and applies circuit laws and power physics to detect anomalies. Jolt operates at both a substation level and a grid level to identify compromised substations and suspicious and misbehaving controllers within a substation.

KEY JOLT BENEFITS

- Employs a new analysis vector to detect attacks on industrial control systems that seek to infiltrate and corrupt telemetry reporting.
- Finds inconsistencies indicative of system misconfiguration or compromise
- Intelligently analyzes and aggregates discrepancies to rank order a list of suspect devices with "trustworthiness" scores
- Performs distributed, multi-level analysis within individual substations and across the grid
- Supports key telemetry SCADA protocols: DNP3/IP, DNP3/Serial, SEL Fast Message/Serial, Modbus TCP, Modbus/Serial, and IEC 61850 Generic Object-Oriented Substation Events (GOOSE)/Ethernet
- Ingests and correlates multiple telemetry sources: relays, RTUs, RTACSs, revenue meters, secondary telemetry, direct relay metering, Phasor Measurement Units, human reporting, and advanced metering infrastructure (AMI)

For distribution automation (DA) systems, Jolt can examine conditions before and after an event to determine if prior conditions warranted the actions that were taken, and whether those actions were successful. For example, Jolt can compare the power factor before an automated capacitor bank engaged to see if the triggering conditions were met, and examine the power factor after the event to see if conditions improved. When used with a one-line diagram, Jolt can infer conditions from multiple nearby and distant reporting devices to detect inconsistencies in voltages, currents, phase angles, and other parameters to identify a device whose reporting is questionable. Jolt can determine if the data reported by an automated capacitor bank is consistent with values reported by other upstream and downstream devices.



Jolt detecting compromised RTAC performing malicious reporting

JOLT'S INNOVATIVE COMPONENTS AND CAPABILITIES

- 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 can be easily extended to model and protect other control systems (e.g., utilities, manufacturing, materials processing)

COMPARING JOLT TO OTHER TOOLS

Cybersecurity tools employed in ICS and power system applications typically reside in a gateway and offer traditional IT capabilities such as IP traffic analysis and IT protocol analysis for web-based protocols. Jolt is a revolutionary cybersecurity tool using a new analysis vector that analyzes substation telemetry. Jolt rapidly detects misreporting devices and system configuration errors. It identifies suspicious, and potentially compromised, devices by analyzing inconsistencies in grid state telemetry to detect stealthy and complex cyberattacks.

For more information on Jolt and Peraton Labs solutions for the energy sector, see Energy - Peraton Labs or contact info@peratonlabs.com.

Peraton