PROTOCOLPATROLLER

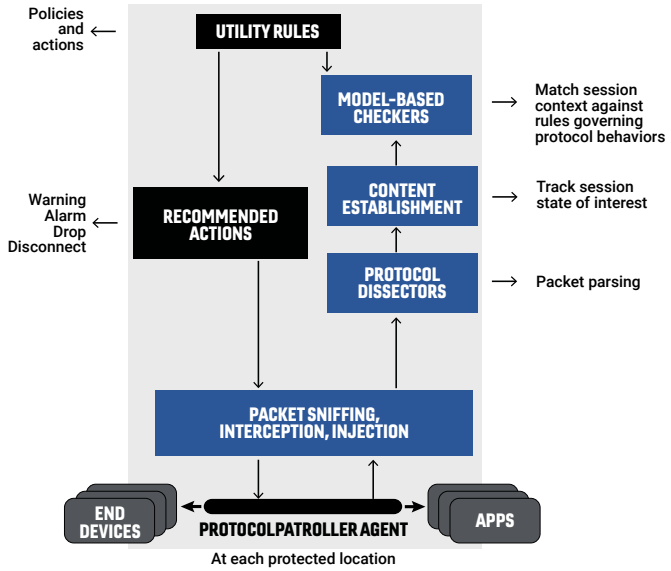
An All-In-One SCADA Cybersecurity and Operations Support Solution

INTRODUCTION TO PROTOCOLPATROLLER

ProtocolPatroller is an all-in-one solution, providing both cybersecurity and operations support for Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems.

As part of Peraton Labs' EnergyDefender cyber integrity solution for critical infrastructure, ProtocolPatroller performs real-time SCADA communication session mapping and protocol analysis. Its uses stateful model-based protocol checkers to analyze session communications and protocol operations and to detect packet and session anomalies, sensitive operations, and events of concern using built-in and operator-defined rules.

For operations support, ProtocolPatrolller provides visibility into Remote Terminal Unit (RTU)-endpoint communications to reduce time to resolution for troubleshooting, fixing configuration errors, and validating new system deployment. With ProtocolPatroller, customers get an industry-leading cyber defense capability for their Security Operations Center (SOC), plus a multi-purpose solution, delivering daily benefit to process control, engineering, and protection teams.



PROTOCOLPATROLLER FEATURES

- A purpose-built SCADA cybersecurity and operations support solution
- Detects protocol session anomalies using stateful model-based checkers and operator defined rules
- Performs real-time, multi-level session mapping, visualization, and node tracking from layer 2 through SCADA application layer
- Overcomes the serial "blind spot" problem and supports analysis of non-Internet Protocol (IP) SCADA traffic
- Alerts on sensitive operations, engineering access, privileged access attempts, and events that could negatively affect process control
- Deploys in a monitor-only or active defense/ intervention mode for advanced operator control and SCADA system recovery
- Automatically recognizes protocols based on protocol data packet specifics, even when protocols use non-standard ports

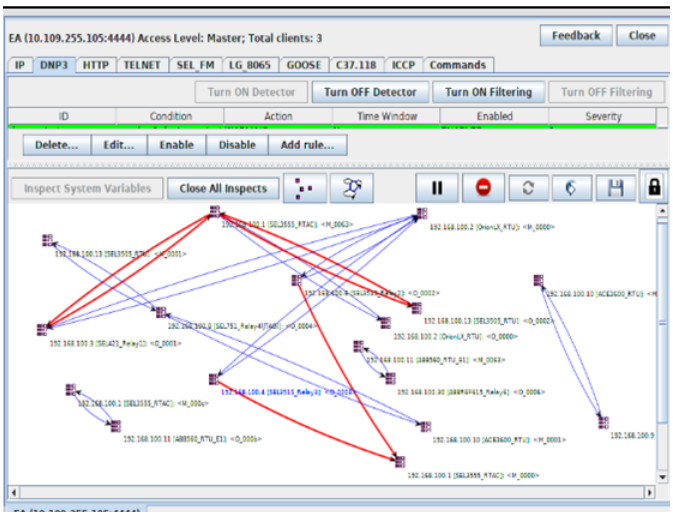
HOW PROTOCOLPATROLLER WORKS

ProtocolPatroller consists of a packet analysis agent and a client user application. Multiple instances of the agent are deployed at different infrastructure vantage points to monitor process and network-level communications. The user selects an inspection point via the client user application. ProtocolPatroller converts the communications session information between each source and destination pair from the inspection point to create a real-time, current-state view of the logical communications flows. Each node is labeled by its familiar name, IP address, protocol role, and protocol ID.

Drilldown capabilities provide detailed information for each session. Unrecognized devices detected in the environment and sessions with anomalies are highlighted for easy visibility. To support large and complex environments, ProtocolPatroller provides the ability to display specific subnets.

Multi-level Session Mapping

A powerful feature of ProtocolPatroller is its ability to map sessions at multiple layers in the protocol stack and show layered connection relationships at the SCADA level. Many SCADA protocols were originally designed for serial connections and later encapsulated within IP for routable network transport. ProtocolPatroller simultaneously tracks sessions at both the SCADA protocol level and the IP level and can discern logical channels using the same IP address pair. ProtocolPatroller not only maps the Transmission Control Protocol (TCP) communications between an RTU and SCADA endpoint at the IP level, but also maps the DNP3 master-outstation flows between each DNP3 ID pair at the DNP3 layer.



Serial and Non-IP Traffic Support

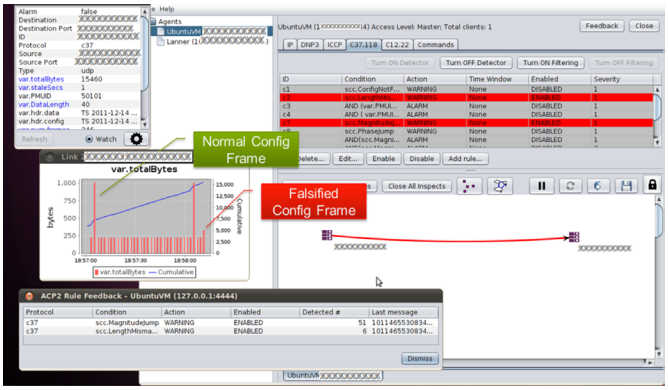
Another key feature of ProtocolPatroller is support for non-IP SCADA communications. ProtocolPatroller tracks and analyzes layer 2 Ethernet and serial SCADA protocols just as easily as native IP-based protocols. Protocols, such as 61850 Generic Object-Oriented Substation Events (GOOSE) are process level protocols that replace physical control wiring in modern SCADA environments. GOOSE is a layer 2 protocol dropped directly into an Ethernet frame without IP services. ProtocolPatroller treats it as just another protocol for mapping and analysis.

ProtocolPatroller provides a solution for the serial “blind spot” problem in ICS infrastructure. Most ICS monitoring systems focus solely on IP traffic. In combination with Peraton Labs’ EnergyDefender™ sensors, ProtocolPatroller also maps and analyzes serial communications. For instance, ProtocolPatroller can map serial sessions using Schweitzer Engineering Laboratories (SEL) Fast Message sessions between a Real Time Automation Controller (RTAC) or communications processor and relay systems much the same way IP connections are mapped for IP-based Distributed Network Protocol 3 (DNP3) sessions.

Access and Sensitive Operations Alerting

ProtocolPatroller analyzes SCADA protocol payloads, in addition to port and connection information. Using a rules-based engine, ProtocolPatroller will alert not only on protocol violations and irregularities, but also on privileged and sensitive operations, according to user configured rules.

ProtocolPatroller can be configured to alert SOC personnel to equipment engineering access, including access methods which circumvent the gateways and terminal service, that are typically used. ProtocolPatroller can detect and alert on control operations, protocol commands, and sensitive operations that are uncommon in standard SCADA infrastructures.



Major SCADA Protocol Support

ProtocolPatroller provides session analysis and cybersecurity analysis for the major SCADA protocols listed below. It employs a modular architecture that can be readily extended to support additional ICS protocols.

- Distributed Network Protocol (DNP3)
- 61850-Generic Object-Oriented Substation Events (GOOSE)
- Schweitzer Engineering Laboratories (SEL) Fast Message protocol
- Modbus/Modbus TCP
- Inter-Control Center Communications Protocol (ICCP)
- Landis + Gyr 8065
- Synchrophasor Protocol C37.118
- Advanced Metering Infrastructure (AMI) Data Transport Protocol C12.22
- IP Protocols, such as IP, Telnet, Hypertext Transfer Protocol (HTTP), Address Resolution Protocol (ARP)

ProtocolPatroller Modes of Deployment

ProtocolPatroller can be deployed in a passive monitor-only mode or an active defense / intervention mode.

- Monitor-only mode: passively analyzes, detects, and alerts on behavior anomalies using a predefined set of protocol-specific rules and environment parameters
- Active Defense/Intervention: actively intervenes according to prescribed actions to mitigate malicious behavior and terminate sessions
- In the active defense/intervention mode, ProtocolPatroller can perform as an application-level security gateway to implement a temporary operator hold on certain actions, block specified traffic, and terminate sessions to stop the in-progress attacks. In emergency recovery situations, ProtocolPatroller's active defense can help quarantine suspect devices from the network and allow only certain permitted operations or, conversely, protect an enclave of equipment from anomalous activity in the larger network infrastructure.

COMPARING PROTOCOLPATROLLER TO OTHER TOOLS

ProtocolPatroller is an industry leading SCADA cybersecurity and operations support solution that delivers dual benefit in one solution. It supports serial and non-IP protocols, provides an alerting solution for engineering and privileged access, and can intervene under operator direction to operate as a protocol level gateway. ProtocolPatroller is a proven technology that is currently used by leading utility operators to monitor their advanced distribution, ICS, and SCADA systems.

BENEFITS

- Visualize and validate Energy Management System (EMS)/RTU polling hierarchy and master-outstation relationships
- Troubleshoot SCADA reporting problems at application and transport levels.
- Identify network performance problems and unresponsive ICS devices
- Discover unexpected communication flows and devices
- Monitor serial communication links
- Alert on sensitive operations, privileged access and events of interest

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

Peraton