UNITED STATES PATENT AND TRADEMARK OFFICE

Patent No. US11567890

Deep Packet Inspection Engine for Industrial Control Systems

Issue Date: March 15, 2023

Filing Date: April 12, 2021

Priority Date: April 15, 2020

Assignee: DeepShield Systems, Inc.

Inventors: Rodriguez, Elena; Morrison, James; Chen, Marcus

Term: 20 years from filing date

ABSTRACT

A system and method for real-time deep packet inspection of industrial control system network traffic, comprising an adaptive analysis engine that employs machine learning algorithms to detect anomalous patterns in operational technology protocols. The invention includes mechanisms for protocol-aware parsing of industrial communications, behavioral baseline establishment, and automated threat response within critical infrastructure environments.

CLAIMS

A method for deep packet inspection in industrial control systems, comprising:

a) receiving network traffic from industrial control system components;

b) parsing said traffic according to predetermined protocol definitions specific to operational technology environments;

c) analyzing parsed traffic using a machine learning model trained on normal operational patterns;

d) detecting deviations from established behavioral baselines; and

e) initiating automated response actions based on threat classification.

The method of claim 1, wherein the protocol definitions include:

a) Modbus TCP/IP

b) DNP3

c) EtherNet/IP

d) Profinet

e) BACnet

f) S7 Communication

A system for implementing the method of claim 1, comprising:

a) network traffic capture modules deployed at critical infrastructure nodes;

b) a central processing engine incorporating:

- Protocol parsing libraries
- Machine learning model implementation
- Threat classification engine
- Response automation framework

The system of claim 3, further comprising:

a) a distributed architecture for scalable deployment across multiple industrial sites;

b) redundant processing capabilities for high availability;

c) encrypted communication channels between components.

DETAILED DESCRIPTION

Background

Industrial control systems face increasing cybersecurity threats requiring sophisticated detection mechanisms. Traditional packet inspection methods lack the context awareness needed for operational technology environments. This invention addresses these limitations through advanced protocol-aware analysis.

Technical Implementation

The deep packet inspection engine employs a multi-layer architecture:

Protocol Analysis Layer

- Custom protocol dissectors for industrial protocols

- State tracking for protocol sequences
- Command validation against allowed operations

Behavioral Analysis Layer

- Statistical modeling of normal operations
- Pattern recognition for device interactions
- Temporal analysis of command sequences

Machine Learning Layer

- Neural network-based anomaly detection
- Supervised classification of known threat patterns
- Continuous model adaptation based on feedback

Security Features

The system incorporates multiple security mechanisms:

Data Protection

- End-to-end encryption of analysis results
- Secure storage of behavioral baselines
- Access control for configuration changes

Operational Safeguards

- Failsafe modes for critical systems
- Non-intrusive monitoring capabilities
- Configurable response thresholds

DRAWINGS

Figure 1: System Architecture Diagram

Figure 2: Protocol Analysis Workflow

Figure 3: Machine Learning Model Structure

Figure 4: Deployment Configuration Examples

INDUSTRIAL APPLICABILITY

This invention is particularly applicable to:

- Power generation and distribution systems
- Water treatment facilities
- Manufacturing operations
- Oil and gas infrastructure
- Maritime control systems
- Transportation networks

PRIOR ART REFERENCES

US Patent 10234567 - Network Traffic Analysis System

US Patent 10345678 - Industrial Protocol Parser

US Patent 10456789 - Cybersecurity Monitoring System

INVENTOR DECLARATIONS

We, the undersigned inventors, hereby declare that:

We believe we are the original inventors of the claimed invention

We have reviewed and understand the contents of this application

We acknowledge the duty to disclose material information

SIGNATURES

/s/ Dr. Elena Rodriguez

Chief Security Architect

Date: April 12, 2021

/s/ James Morrison

VP of Engineering

Date: April 12, 2021

/s/ Dr. Marcus Chen

Chief Executive Officer

Date: April 12, 2021

PATENT ATTORNEY CERTIFICATION

I hereby certify that this patent application meets all requirements for submission to the USPTO.

/s/ Sarah Johnson

Patent Attorney Reg. No. 65432

Date: April 12, 2021