UNITED STATES PATENT AND TRADEMARK OFFICE

Patent No. US10984562 B2

DeepShield Core Architecture for Industrial Control System Security

Filing Date: March 15, 2019

Issue Date: April 20, 2021

Assignee: DeepShield Systems, Inc., Wilmington, Delaware

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

ABSTRACT

A system and method for providing multi-layered security architecture for industrial control systems (ICS) and operational technology (OT) environments. The invention comprises an AI-driven threat detection engine integrated with real-time monitoring capabilities and automated response mechanisms specifically designed for protecting critical infrastructure components. The architecture implements novel deep-learning algorithms for anomaly detection in SCADA networks while maintaining operational continuity.

CLAIMS

A method for securing industrial control systems, comprising:

a) implementing a multi-layered security architecture comprising:

- a deep packet inspection (DPI) engine optimized for OT protocols
- an AI-based threat detection module
- a real-time monitoring system
- an automated incident response framework

b) wherein said architecture:

- processes network traffic at wire speed
- maintains state awareness of protected systems
- generates behavioral baselines for normal operations
- identifies anomalous patterns without disrupting critical processes

The method of Claim 1, wherein the AI-based threat detection module:

- utilizes proprietary neural network architectures
- maintains continuous learning capabilities
- adapts to evolving threat landscapes
- generates threat intelligence specific to industrial environments

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

- dedicated hardware processors
- specialized firmware
- secure memory modules
- hardened operating system
- encrypted communication channels

DETAILED DESCRIPTION

Background

The present invention addresses critical security challenges in industrial control systems and operational technology environments. Traditional IT security solutions are inadequate for protecting industrial infrastructure due to unique operational requirements and protocols. This invention provides a comprehensive security architecture specifically designed for industrial applications.

Technical Implementation

The core architecture comprises four primary components:

Deep Packet Inspection Engine

- Protocol-aware parsing for industrial protocols
- Zero-copy packet processing
- Hardware-accelerated pattern matching
- Custom protocol decoders for proprietary industrial protocols

AI-Based Threat Detection

- Multi-layer neural network architecture
- Real-time pattern recognition
- Behavioral analysis engine
- Automated threat classification system

Monitoring System

- High-speed telemetry collection
- Distributed sensor network
- Real-time data aggregation
- Performance optimization layer

Response Framework

- Automated threat mitigation
- Configurable response policies
- Integration with existing security infrastructure
- Audit trail generation

Novel Features

The invention introduces several innovative features:

Adaptive Learning System

- Self-evolving threat models
- Dynamic baseline adjustment
- Continuous performance optimization
- Automated rule generation

Industrial Protocol Support

- Native support for Modbus, DNP3, EtherNet/IP
- Custom protocol extension framework
- Protocol normalization layer
- Traffic optimization mechanisms

Security Mechanisms

- Hardware-based encryption
- Secure boot process
- Trusted execution environment
- Integrity verification system

DRAWINGS

Figure 1: System Architecture Diagram

Figure 2: Component Interaction Flow

Figure 3: Protocol Stack Implementation

Figure 4: Security Layer Integration

Figure 5: Deployment Topology

INDUSTRIAL APPLICABILITY

This invention is particularly applicable to:

- Critical infrastructure protection
- Industrial automation systems
- SCADA networks
- Manufacturing operations
- Maritime facilities
- Offshore platforms
- Energy distribution systems

LEGAL NOTICES

The technical information contained herein is considered confidential and proprietary to DeepShield Systems, Inc. Any use of the described methods and systems requires explicit written permission from the patent holder.

CERTIFICATION

I hereby certify that I am authorized to execute this patent application on behalf of DeepShield Systems, Inc.

/s/ Dr. Marcus Chen

Chief Executive Officer

DeepShield Systems, Inc.

Date: March 15, 2019

/s/ Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: March 15, 2019