OT ASSET DISCOVERY PROTOCOL

United States Patent No. US11345678

TITLE OF INVENTION

System and Method for Automated Discovery and Classification of Operational Technology Assets in Industrial Control Networks

ABSTRACT

A system and method for discovering, identifying, and classifying operational technology (OT) assets in industrial control system networks using passive network monitoring and machine learning-based fingerprinting techniques. The invention comprises methods for protocol-agnostic traffic analysis, device behavior profiling, and automated asset classification without requiring active network scanning or system modifications.

BACKGROUND OF INVENTION

This invention relates to the field of industrial cybersecurity, specifically addressing the challenges of identifying and maintaining accurate inventories of operational technology assets in critical infrastructure environments. Traditional IT-based asset discovery methods are often unsuitable for OT environments due to the sensitive nature of industrial control systems and the risk of disruption from active scanning techniques.

DETAILED DESCRIPTION

1. System Overview

1 The system comprises:

(a) Network traffic capture modules deployed at strategic points within an industrial control network

(b) A central processing engine implementing proprietary machine learning algorithms

(c) A secure database for storing device fingerprints and classification data

(d) An API interface for integration with existing asset management systems

2 The system operates by:

(a) Passively monitoring network communications

(b) Extracting device characteristics from observed traffic patterns

(c) Comparing extracted characteristics against known device profiles

(d) Generating unique device fingerprints for identified assets

2. Asset Discovery Method

1 The method includes the following steps:

(a) Initial passive network observation period of 24-168 hours

(b) Protocol identification and traffic pattern analysis

(c) Device behavior profiling using proprietary algorithms

(d) Automated classification based on observed characteristics

(e) Continuous monitoring for network changes

2 Classification parameters include:

(a) Communication protocols utilized

(b) Traffic patterns and timing characteristics

(c) Device response behaviors

(d) Protocol-specific attributes

(e) Vendor-specific identifiers

3. Machine Learning Implementation

1 The system employs multiple machine learning models:

(a) Supervised learning for known device classification

(b) Unsupervised learning for anomaly detection

(c) Deep learning for protocol analysis

(d) Reinforcement learning for classification optimization

2 Training data comprises:

(a) Labeled device profiles from controlled environments

(b) Anonymized traffic patterns from production networks

(c) Vendor-provided device specifications

(d) Historical classification results

4. Security Measures

1 The system implements the following security controls:

(a) Encrypted storage of all collected data

(b) Role-based access control for system functions

(c) Audit logging of all system activities

(d) Secure communication channels for data transmission

5. Integration Capabilities

1 The system supports integration with:

(a) Industrial control system networks

(b) SCADA systems

(c) Manufacturing execution systems

(d) Enterprise asset management platforms

CLAIMS

A method for discovering operational technology assets in industrial networks comprising:

- Passive network monitoring without active scanning
- Machine learning-based device fingerprinting
- Automated asset classification
- Continuous network observation
- Real-time inventory updates

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

- Network traffic capture modules
- Central processing engine
- Secure database
- Integration API
- User interface

INVENTORS

- Dr. Elena Rodriguez
- James Morrison
- Sarah Blackwood

ASSIGNEE

DeepShield Systems, Inc.

1234 Innovation Drive

Wilmington, Delaware 19801

PATENT DETAILS

Filing Date: March 15, 2022

Issue Date: September 22, 2023

Priority Date: March 15, 2022

Patent Term: 20 years from filing date

LEGAL REPRESENTATION

Wilson & Patterson LLP

Patent Registration No. 12345

This patent document contains confidential and proprietary information of DeepShield Systems, Inc. All rights reserved. Unauthorized reproduction or distribution is prohibited.

[END OF PATENT DOCUMENT]