EUROPEAN PATENT SPECIFICATION

EP3912345 B1

DEEPSHIELD ENCRYPTION MODULE FOR INDUSTRIAL CONTROL SYSTEMS

Publication Date: 15 March 2023

Application Number: EP21234567.8

Filing Date: 12 January 2021

Priority Date: 15 January 2020 (US 63/159,876)

[54] Title of Invention

Method and System for Real-Time Encryption of Industrial Control System Communications Using Adaptive Key Generation

[72] Inventors

RODRIGUEZ, Elena; MORRISON, James; CHEN, Marcus

[73] Proprietor

DeepShield Systems, Inc.

1234 Innovation Drive

Wilmington, Delaware 19801

United States of America

[57] Abstract

A system and method for securing industrial control system communications through dynamic encryption key generation and management. The invention comprises a novel approach to protecting operational technology (OT) networks through real-time adaptive encryption that responds to detected threat patterns. The system utilizes machine learning algorithms to optimize key generation parameters based on network behavior analysis and implements a multi-layer encryption protocol specifically designed for SCADA and ICS environments.

Technical Field

[0001] The present invention relates to cybersecurity systems for industrial control networks, and more particularly to encryption methods for protecting communications in operational technology environments including SCADA systems, programmable logic controllers (PLCs), and related industrial automation infrastructure.

Background

[0002] Industrial control systems face increasing cybersecurity threats that can compromise critical infrastructure operations. Traditional encryption methods often prove inadequate for the unique requirements of OT networks, particularly regarding latency constraints and real-time processing needs.

[0003] Existing solutions typically employ static encryption protocols that fail to adapt to emerging threats and changing network conditions. There remains a need for dynamic encryption systems specifically optimized for industrial control environments.

Summary of Invention

[0004] The present invention provides an adaptive encryption module that generates and manages encryption keys based on real-time analysis of network behavior and threat patterns. The system comprises:

a) A neural network-based threat detection engine that continuously monitors network traffic patterns;

b) An adaptive key generation algorithm that dynamically adjusts encryption parameters based on detected threat levels;

c) A distributed key management system optimized for industrial control system architectures;

d) Real-time encryption/decryption modules with latency optimization for OT environments.

Detailed Description

[0005] The encryption module implements a novel approach to securing industrial control system communications through:

Key Generation

[0006] The system utilizes a proprietary algorithm for generating encryption keys based on:

- Network behavior analysis
- Threat pattern detection
- System state parameters
- Environmental conditions

Adaptive Response

[0007] The encryption parameters automatically adjust based on:

- Detected threat levels
- Network performance metrics
- System resource utilization
- Critical operation requirements

Implementation Architecture

[0008] The system comprises:

- Central key management server
- Distributed encryption nodes
- Real-time monitoring modules
- Adaptive configuration engine

Claims

A method for securing industrial control system communications comprising:

a) Monitoring network traffic patterns using neural network analysis;

b) Generating encryption keys based on detected threat patterns;

c) Implementing adaptive encryption parameters;

d) Managing key distribution across OT networks.

The method of claim 1, wherein the neural network analysis comprises:

a) Real-time traffic pattern analysis;

b) Threat signature detection;

c) Anomaly identification;

d) Risk level assessment.

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

a) Network monitoring modules;

b) Key generation engine;

c) Encryption parameter management system;

d) Distribution control mechanism.

Description of Drawings

[0009] Figure 1: System architecture diagram

[0010] Figure 2: Key generation process flow

[0011] Figure 3: Adaptive response mechanism

[0012] Figure 4: Implementation schema

Industrial Applicability

[0013] The invention provides significant advantages for securing industrial control systems through:

- Reduced latency impact
- Enhanced threat responsiveness
- Optimized resource utilization
- Improved operational reliability

Patent Declarations

[0014] The proprietor has declared that this European patent is subject to licensing under FRAND (Fair, Reasonable, And Non-Discriminatory) terms for essential implementations in industrial control system security standards.

Authorization

Executed this 15th day of March, 2023

/s/ Elena Rodriguez

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

/s/ James Morrison

James Morrison

VP of Engineering

DeepShield Systems, Inc.

European Patent Office Reference: EP3912345

Classification: G06F 21/60, H04L 9/08