EUROPEAN PATENT SPECIFICATION

EP3901234 B1

DEEPSHIELD MULTI-FACTOR AUTHENTICATION SYSTEM FOR INDUSTRIAL CONTROL NETWORKS

Patent Proprietor: DeepShield Systems, Inc.

Filing Date: March 15, 2019

Publication Date: September 22, 2020

Grant Date: January 12, 2021

DESCRIPTION

[0001] Technical Field

The present invention relates to authentication systems for industrial control networks, and more particularly to a multi-factor authentication system utilizing behavioral biometrics and contextual analysis for securing access to operational technology (OT) environments.

[0002] Background

Industrial control systems face increasing cybersecurity threats requiring robust authentication mechanisms beyond traditional password-based approaches. Existing solutions fail to adequately address the unique challenges of OT environments where standard authentication methods may interfere with critical operations.

[0003] Summary of the Invention

The invention provides a novel authentication system specifically designed for industrial control networks that combines:

- Behavioral biometric analysis of operator interaction patterns
- Contextual validation of access requests based on operational parameters
- Adaptive risk scoring incorporating environmental sensors
- Non-disruptive continuous authentication

[0004] Detailed Description

Authentication System Architecture

The system comprises:

A central authentication server

Distributed sensor nodes

Behavioral pattern analysis engine

Context evaluation module

Risk scoring engine

Policy enforcement point

Behavioral Biometric Components

The system captures and analyzes:

- Keyboard dynamics
- Mouse movement patterns
- Command sequence patterns
- Interface navigation behaviors
- Temporal access patterns

Contextual Analysis Framework

Authentication decisions incorporate:

- Physical location validation
- Time-of-day correlation
- Operation type classification
- System state evaluation
- Environmental sensor data

[0005] Claims

A method for authenticating access to industrial control systems comprising:

a) Capturing operator behavioral patterns through distributed sensors

b) Analyzing behavioral biometrics against stored profiles

c) Evaluating contextual parameters of access requests

d) Generating dynamic risk scores

e) Enforcing granular access policies

The method of claim 1 wherein behavioral patterns include:

- Keystroke dynamics
- Mouse movement characteristics
- Command sequence patterns
- Interface navigation behaviors
- Temporal access patterns

The method of claim 1 wherein contextual parameters include:

- Physical location data
- Temporal correlation
- Operation classification
- System state
- Environmental conditions

[Claims 4-20 omitted for brevity]

[0006] Abstract

A multi-factor authentication system for industrial control networks utilizing behavioral biometrics and contextual analysis. The system combines continuous behavioral monitoring, environmental sensing, and adaptive risk scoring to provide secure, non-disruptive authentication for operational technology environments.

[0007] Drawings

[Figure references omitted for brevity]

[0008] Patent Family Information

- PCT Application: PCT/US2019/022445
- Priority Date: March 15, 2019
- Related Applications: US16/354,789

[0009] Designated Contracting States

AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LI, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR

[0010] Proprietor Details

DeepShield Systems, Inc.

1234 Innovation Drive

Wilmington, Delaware 19801

United States of America

[0011] Inventors

- Chen, Marcus
- Rodriguez, Elena
- Morrison, James
- Blackwood, Sarah

[0012] Representative

Patent Attorneys & Associates LLP

European Patent Attorneys

London EC4A 1EN

United Kingdom

[0013] Legal Notices

[END OF DOCUMENT]