UNITED STATES PATENT AND TRADEMARK OFFICE

PROVISIONAL PATENT APPLICATION

MULTI-DOMAIN AUTHENTICATION AND AUTHORIZATION SYSTEM WITH CREDENTIAL PORTABILITY FOR AI AGENT NETWORKS

INVENTOR: Brian James Rutherford

CITIZENSHIP: United States of America

RESIDENCE: Wimberley, Texas 78676

FILING DATE: [DATE]

APPLICATION NUMBER: [TO BE ASSIGNED]

FIELD OF THE INVENTION

This invention relates to identity and access management systems for MWRASP (Total) defensive cybersecurity platforms, specifically to methods for authenticating AI agents and users across multiple security domains with different trust models and credential requirements in enterprise protection environments.

BACKGROUND OF THE INVENTION

In defensive cybersecurity systems employing AI agents, organizations operate across multiple security domains including on-premises, cloud, partner networks, and customer environments. Each domain typically requires separate credentials for AI agents and users, leading to credential proliferation, increased security risk, and poor operational efficiency. Federation solutions like SAML provide limited interoperability and create single points of failure for AI agent authentication.

Current approaches cannot handle domains with conflicting security requirements for AI agents, different assurance levels for various agent types, or incompatible credential types across agent platforms. No system provides true credential portability with privacy preservation and regulatory compliance across arbitrary domains for both AI agents and human operators in MWRASP (Total) environments.

SUMMARY OF THE INVENTION

The present invention provides a universal authentication system enabling AI agents and users to authenticate once and access resources across any security domain within the MWRASP (Total) platform. The system translates between different credential types, maintains privacy through selective disclosure, and ensures compliance with each domain's security policies while enabling seamless AI agent operations across organizational boundaries.

DETAILED DESCRIPTION OF THE INVENTION

System Architecture

The cross-domain authentication system for AI agent networks implements several innovative components:

Universal Identity Abstraction: The system creates an abstract identity layer independent of any specific domain for both AI agents and human operators. Each AI agent has a universal identifier (UID) derived from cryptographic keys and operational parameters using privacy-preserving hashing. Human users have UIDs based on biometric templates. The UID links to domain-specific identities through encrypted mappings that prevent correlation across domains. Zero-knowledge proofs enable identity verification without revealing the UID.

Credential Translation Engine: The system translates between diverse credential types used by different AI agent platforms including API keys, certificates, OAuth tokens, hardware security modules, and behavioral patterns. Translation occurs through secure multiparty computation where no single party sees all credentials. The engine maintains semantic equivalence ensuring security properties are preserved across translations for both agent and human credentials.

Trust Bridge Protocol: Domains with different trust models for AI agents connect through trust bridges that negotiate minimum acceptable assurance levels for agent operations, map between different authentication factors for various agent types, and provide attestations about authentication events. The protocol handles trust level elevation when AI agents access higher-security domains and graceful degradation for lower-security domains.

Privacy-Preserving Attribute Exchange: AI agents and users selectively disclose attributes required by each domain using attribute-based credentials. Cryptographic commitments prove attribute possession without revealing values. For example, an AI agent proving security clearance level without revealing specific classification, or proving operational authority without revealing specific permissions.

Continuous Authentication Framework: The system implements continuous authentication for AI agents through behavioral biometrics including API call patterns, resource usage characteristics, and operational decision patterns. Machine learning models create agent-specific baselines updated through online learning. Anomaly detection triggers step-up authentication when agent behavior deviates from baseline.

Regulatory Compliance Engine: The system ensures compliance with regulations across all domains for AI agent operations through policy expression in formal logic, automated policy conflict resolution for agent permissions, and audit trail generation with cryptographic integrity. Compliance proofs are generated using zero-knowledge techniques, proving agent compliance without exposing sensitive operational data.

Session Management Across Domains: The system maintains secure sessions for AI agents across domain boundaries through distributed session state with Byzantine fault tolerance, automatic session migration during domain transitions, and coordinated session termination across all domains. Agent sessions include replay protection and perfect forward secrecy.

The invention enables authentication across 100+ domains simultaneously for AI agent fleets, sub-second authentication with cached credentials, support for 50+ credential types including agent-specific formats, and zero correlation between domains for privacy. Applications include multi-

cloud AI agent deployments, healthcare information exchange with AI agents, financial services integration using security agents, and government federated systems with AI agent participation.

CLAIMS

1. A cross-domain authentication system for AI agent networks comprising:

universal identity abstraction for AI agents and users;

credential translation engine supporting multiple credential types;

trust bridge protocol connecting domains with different trust models;

privacy-preserving attribute exchange mechanism;

wherein said system enables single sign-on across multiple domains.

2. The system of claim 1, supporting authentication across 100 or more domains simultaneously.

3. The system of claim 1, wherein said translation engine uses secure multiparty computation.

4. The system of claim 1, further comprising continuous authentication based on AI agent behavioral patterns.

5. The system of claim 1, including zero-knowledge proofs for identity verification.

6. A method for cross-domain authentication of AI agents comprising:

creating universal identifiers for AI agents;

translating credentials between domain-specific formats;

establishing trust bridges between domains;

selectively disclosing agent attributes;

maintaining continuous authentication through behavioral analysis.

7. The method of claim 6, achieving sub-second authentication latency.

8. The method of claim 6, wherein said behavioral analysis uses machine learning for anomaly detection.

9. A computer-readable medium containing instructions for cross-domain AI agent authentication.

10. The system of claim 1, integrated within a MWRASP (Total) defensive cybersecurity platform.

ABSTRACT

A multi-domain authentication and authorization system enabling AI agents and users to seamlessly operate across different security domains with varying trust models. The system provides universal identity abstraction, credential translation, trust bridging, and privacy-preserving attribute exchange while maintaining continuous authentication through behavioral analysis. Essential for MWRASP (Total) platforms requiring AI agents to coordinate protection across organizational and technical boundaries.