Agentic-ZTA: Rethinking Autonomous Zero Trust Through Agentic AI

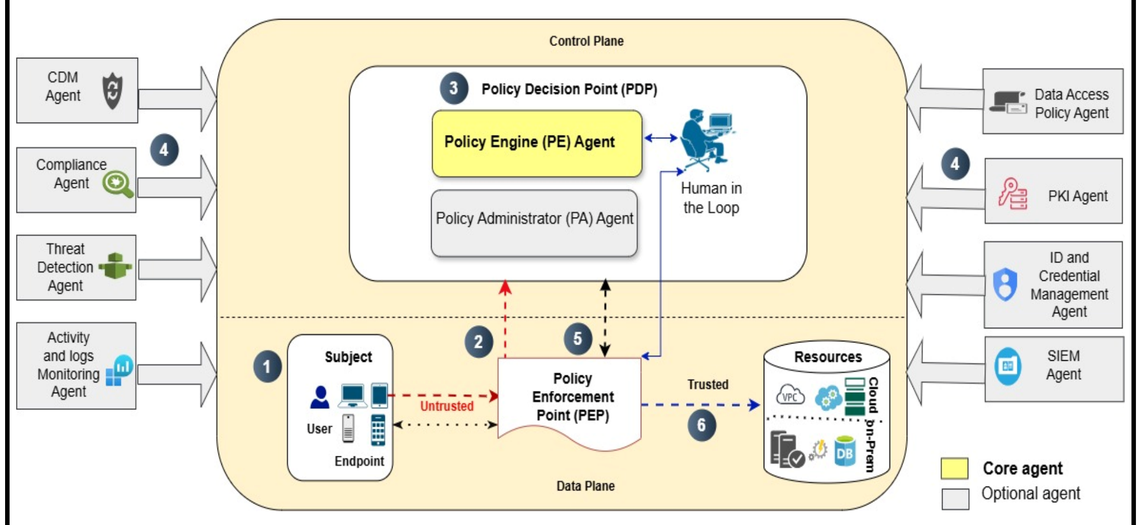
Problem Statement and Goals

Zero Trust Architecture is grounded on the principle “Never Trust, Always Verify”. However, traditional ZTA implementations rely on a stable, centralized infrastructure to validate every access request. In a battlefield scenario, central authority becomes a single point of failure. If the link to the central command is disrupted, the verification process collapse, turning conventional ZTA into a critical vulnerability.

Goal: This paper introduces an Agentic AI based Zero Trust Architecture (Agentic-ZTA), where NIST Zero Trust principles are enforced by the AI agents, agents are embedded on edge devices to serve as localized, autonomous Policy Decision Points.

Approach

Agentic-ZTA Architecture



Results

Results:

The Agentic-ZTA framework envisions a future where zero trust architecture are not merely deployed but autonomously enforced by AI agents. This paradigm shift replaces static, rule-based policy enforcement with dynamic, context-aware, and agentic decision-making. However, high-impact decisions are subject to human in the loop policies enforced by the policy engine agent.

Future work:

- Testbed Implementation
- Agent development and deployment
- Agent security
- Uncertainty quantification

Acknowledgments:

- Team Members: Shovan Roy, Lopamudra Praharaj, Deepti Gupta, Maanak Gupta

Shovan Roy
Tennessee Tech University

Agentic-ZTA: Rethinking Autonomous Zero Trust Through Agentic AI

Abstract

The rise of Large Language Models (LLMs) has created new era for AI driven cybersecurity. As cyber threats become increasingly sophisticated, the need for autonomous intelligent systems to identify vulnerabilities, analyze attack pattern and manage risk in real-time increases. LLMs can enhance vulnerability detection, malware analysis, intrusion detection, phishing detection, and policy interpretation. However, they lack the autonomous decision-making and action capabilities required for real-time proactive enforcement. Agentic AI, by creating a topology of LLM-based reasoning with autonomous decision-making and action taking capabilities, overcome these limitations.

Zero-Trust Architecture (ZTA) enforces strict access controls by default, operating on the principle that no entity, whether users, IoT devices, or services should be trusted implicitly, instead, access to resources is granted on a per-request basis, ensuring that only necessary actions are permitted and lateral movement is minimized.

This research re-architect Zero Trust as a self organizing multi-agent system, where each zero trust function is enforced by the autonomous AI agents. Agentic-ZTA framework integrates autonomous contextual agents, which provide fine-grained access control, real-time threat detection, and dynamic policy adaptation with symbolic reasoning. In addition, a trust algorithm aggregates input from specialized agents to create a dynamic trust score, to resolve conflicting decisions. Our proposed autonomous Agentic AI based Zero Trust architecture (Agentic-ZTA) explores an innovative solution to modern cybersecurity challenges and demonstrates its utility by providing a fully integrated agent coordination and automated response for zero trust enforcement in a dynamic contested environment.

Shovan Roy
Tennessee Tech University