MORGAN STATE UNIVERSITY

Development of a Unified Theoretical Framework

for Zero Trust Enterprise Network Cybersecurity (ZTENS)

Olufemi Agunbiade | Dr. Onyema Osuagwu • The C4 Lab, Morgan State University, Maryland

CAE CONFERENCE 2026

Abstract

Zero Trust Cybersecurity (ZTCS) represents a fundamental paradigm shift toward continuous verification and eliminating implicit trust. While widely adopted across industry and government, the field lacks a cohesive theoretical framework for implementing, measuring, and comparing Zero Trust Architecture (ZTA) effectiveness.

This research addresses this gap by developing a unified mathematical framework for Zero-Trust Enterprise Network Security (ZTENS) using measurement-driven theory and quantitative methods to evaluate an enterprise network ZT level.

Keywords: *Zero Trust Architecture, enterprise network security, trust metrics, quantitative evaluation, security maturity models, cybersecurity education*

Motivation & Problem Statement

- ZTA widely adopted in industry & government — but lacks rigorous mathematical foundations.
- No unified metric exists to measure, compare, or benchmark Zero Trust effectiveness across organizations.
- Current implementations rely on qualitative checklists rather than quantitative trust evidence.
- Cybersecurity curricula lack quantitative foundations for teaching Zero Trust principles at the graduate level.
- This work develops a formal, measurement-driven ZTENS framework to close these gaps.

Key Theoretical Contributions

System Model Z
Formal state-transition model Z = (E, C, S, A, T, I, P, Y) defining all ZT system components.

Session Trust Estimation
Bayesian Beta model with decay: posterior trust T_t = A_t/(A_t+B_t) updated from calibrated telemetry signals.

Minimal-Trust System (MTS)
Absolute zero-risk ZT is unachievable. MTS minimizes implicit trust through continuous calibrated verification.

Zero Trust Maturity Index
ZTMI: quantitative metric measuring proximity to minimal-trust boundary across enterprise architectures.

Education Impact

This framework advances

- Quantitative foundations for teaching Zero Trust at graduate level
- Lab simulations of trust-score computation and verification policies
- Real enterprise telemetry-based maturity assessment exercises
- Bridges theory and practice for cybersecurity professionals

Methodology

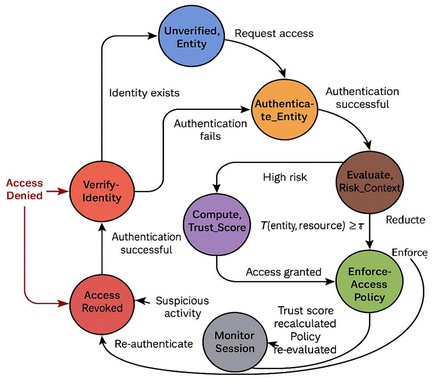
1. **Formal System Modeling**
   Define ZTENS as state-transition system Z with entities, context, actions, and security policy constraints.
2. **Trust Signal Extraction**
   Telemetry X_t ∈ $\mathbb{R}^m$ captures identity, device, behavioral, network, environmental, and policy features.
3. **Calibrated Likelihood:** Logistic mapping y_t = σ(b₀ + bᵀX_t) converts raw features to probability in [0,1], and maps telemetry to calibrated legitimacy likelihood.
4. **Bayesian Trust Update**
   Beta conjugate model with exponential decay (ρ = e^{−λδ}) yields adaptive posterior trust T_t.
5. **ZTMI Scoring:** Aggregate posterior trust scores benchmarked across 10 enterprise networks.

System Model Definition — State-Transition Framework

The enterprise Zero Trust system is formally defined as a 7-tuple state-transition model: Z = (E, C, S, A, T, I, P, Y)

where:

- $\boldsymbol{E}$ = Set of entities interacting within the network (e.g., Users/Roles u ∈ U, devices/edge systems d ∈ D, resources r ∈ R, sessions s.).
- **C** = Context/telemetry is the observed feature vector at discrete time *t*:
  $$\boldsymbol{X_t} = [\boldsymbol{X_t^{id}}, \boldsymbol{X_t^{device}}, \boldsymbol{X_t^{net}}, \boldsymbol{X_t^{beh}}, \boldsymbol{X_t^{geo}}, \dots]$$
- $\boldsymbol{S}$ = Set of possible system states (e.g., user authentication states, device management categories, access levels, network states).
- $\boldsymbol{A}$ = Set of allowed actions (e.g., login attempts, access request types)
- $\boldsymbol{T}$: $\boldsymbol{S} \times \boldsymbol{A} \rightarrow \boldsymbol{S}$ = State transition function defining how actions modify system states throughout the entire system evolution.
- $\boldsymbol{I} \subseteq \boldsymbol{S}$ = Set of initial states (valid system starting configurations).
- $\boldsymbol{P}$ = Set of security policies governing the system (e.g., continuous authentication, least privilege)
- $\forall \boldsymbol{s} \in \mathbf{S}, \forall \boldsymbol{a} \in \boldsymbol{A},\ \boldsymbol{T}(\boldsymbol{s}, \boldsymbol{a}) \models \mathbf{P}$ (This ensures all actions conform to Zero Trust principles at every stage)
- $\mathbf{Y} \in \{\boldsymbol{legit}, \boldsymbol{adversary}\}$ = Legitimacy variable



Zero-Trust Security System as a State-Transition Model

Fig. 1: State-transition model ZTENS showing identity verification, trust computation, risk evaluation, policy enforcement, and revocation in continuous ZT control.

Session-Level Latent Trust Computation & Observable Likelihood

*Legitimacy is formulated as a latent variable $\boldsymbol{\Theta}_{s,t} \in [0,1]$ for session **s** at time t, and updated via Bayesian inference from telemetry evidence.*

Latent legitimacy and information set

$\boldsymbol{\mathcal{F}_t}$ ⟹ (current and past telemetry, policy decisions, step−up results, etc)
Telemetry Features $\mathbf{X}_t \in \mathbb{R}^m = [x_{id}, x_{dev}, x_{beh}, x_{net}, x_{env}, x_{pol}, x_{ip}]^\top$

Calibrated likelihood signal & Assurance Mass

Feature vector X_t is mapped to a calibrated Likelihood signal

$$\mathbf{y_t} \in [0,1] = \sigma\,(b_0 + b^\top X_t),$$

where: $\sigma\,(z) = \dfrac{1}{1+e^{-z}}$ (Logistic link)

- $b \in \mathbb{R}^m$ is the weight vector (usually a column).
- $\mathbf{X}_t \in \mathbb{R}^m$ is the feature vector at time ***t***.
- $b^\top X_t$ is the **dot (inner) product** of the vectors: $b^\top X_t = \sum_{i=1}^{m} b_i\, x_{t,i}$

Assurance Mass injected at time *t*.

$$\boldsymbol{\eta t} = \sum_{i=1}^{m} a_i v_i(x_{t,i}),\ a_i \in [0,1],\ v_i\left(x_{t,i}\right) \in [0,1]$$

Bayesian trust state (Beta model with decay)

Conjugate Prior/Memory, $Beta(A_t, B_t).\ A_t, B_t > 0$

$A_1 = \kappa\,\pi_0,\ B_1 = \kappa\,(1-\pi_0),\ \pi_0 \in [0,1], \kappa > 0$

Evidence Update (with decay).

$A_{t+1} = (1-\rho)A_t + \eta t\ y_t,$

$B_{t+1} = (1-\rho)B_t + \eta t\ (1-y_t),$

Decay Parameter $\rho \in (0,1).$

$\boldsymbol{\rho} = e^{-\lambda\delta},$

$\lambda =$ *decay constant*

Posterior Trust

Posterior Trust.

$$\boldsymbol{T_t} = \mathbb{E}[\boldsymbol{\Theta}_{s,t} \mid \boldsymbol{\mathcal{F}_t}] = \frac{A_t}{A_t + B_t} \in [0,1],$$

Fig. 2: Bayesian session-trust model converting telemetry features to calibrated likelihood, weighted by assurance mass, with recursive decay update.

Core Mathematical Framework

Telemetry Feature Vector
$X_t = [x_{id}, x_{dev}, x_{beh}, x_{net}, x_{env}, x_{pol}, x_{ip}]^\top \in \mathbb{R}^m$

Calibrated Likelihood Signal
$y_t = \sigma(b_0 + b^\top X_t),\ \ \sigma(z) = 1 / (1 + e^{-z})$

Assurance Mass (Evidence Weight)
$\eta_t = \Sigma_i\ a_i v_i(x_{t,i}),\ \ a_i \in [0,1],\ \ v_i \in [0,1]$

Decay Parameter
$\rho = e^{-\lambda\delta},\ \ \lambda =$ decay constant, $\ \delta =$ time elapsed

Bayesian Update (Beta Model)
$A_{t+1} = (1-\rho)A_t + \eta_t \cdot y_t$
$B_{t+1} = (1-\rho)B_t + \eta_t \cdot (1-y_t)$

Posterior Trust Score
$T_t = E[\theta_{s,t} \mid F_t] = A_t / (A_t + B_t) \in [0,1]$

Dataset Summary

Organizations: 10 enterprise networks

Sources: IAM, EDR/XDR, SIEM, Firewall, VPN, NAC, UEBA, Policy logs

Features: Identity · Device · Behavior · Network · Environment · Policy

Outputs: Calibrated likelihood y_t · Posterior trust T_t · Enterprise ZTMI

Observation Window: 3–6 months per organization

Privacy: Pseudonymized identifiers, controlled research access

Results & Findings

Zero Trust Maturity Index (ZTMI) — 10 Enterprise Networks

Fig. 3: Cross-enterprise ZTMI comparison showing how authentication strength, device posture, telemetry freshness, and automation drive score variation.

- Strong authentication mechanisms significantly improve ZTMI scores.
- Frequent telemetry collection and automated policy enforcement are critical drivers.
- Weak device posture markedly reduces overall trust maturity.
- Scores ranged from 0.35 (partial ZT) to 0.88 (near-complete ZT adoption).

Conclusions

This framework establishes the first unified mathematical foundation for ZTENS, enabling rigorous trust measurement, organizational benchmarking via ZTMI, and quantitative cybersecurity education. Future work will extend to multi-domain federated ZT and real-time telemetry streams.

Implementation & Data Pipeline (*End-to-end research workflow from telemetry collection to trust estimation, policy decision, and enterprise maturity benchmarking).*)

Goal: Transform raw enterprise telemetry into calibrated session trust scores and enterprise-level Zero Trust Maturity Index (ZTMI) values.

Telemetry Sources: Identity · Device · Network · Behavior · Environment · Policy enforcement logs

Feature Vector
X_t = [x_id, x_dev, x_beh, x_net, x_env, x_pol, x_ip]ᵀ — captures authentication strength, device posture, behavioral deviation, network risk, contextual risk, and policy compliance.

Evidence Weighting: η_t = Σᵢ aᵢvᵢ(x_{t,i}) — weights each signal by source reliability and evidential strength.

Data Pipeline
Ingest → Normalize → Sessionize → Feature Engineer → Calibrate Likelihood → Bayesian Update → Policy Enforce → Aggregate ZTMI

Dynamic Trust Update
A_{t+1} = (1−ρ)A_t + η_t y_t, B_{t+1} = (1−ρ)B_t + η_t(1−y_t)
T_t = A_t/(A_t+B_t), ρ = e^{−λδ} (evidence decay)

Policy Decision Logic

0 → 49	Low trust → Deny / Isolate
50 → 79	Medium trust → Step-up Auth
80 → 100	High trust → Allow + Monitor

ZTMI = $\Sigma_k\ w_k\ M_k$, $\Sigma w_k = 1$ — Enterprise Zero Trust Maturity Index

Validation Design

Dataset Scope
10 enterprise networks observed over a multi-month period.

Data Preparation
Logs parsed, deduplicated, time-aligned, sessionized, normalized into common feature schema.

Unit of Analysis
Each record is a session-resource decision event at time t.

Model Evaluation
Calibration and discrimination metrics; posterior trust evaluated on risk detection, false accepts, and adaptive policy triggering.

Ground Truth
Derived from analyst-reviewed incidents, policy outcomes, malware detections, anomalous activity, and threat intelligence matches.

Comparative Benchmarking
Framework vs. static access rules, checklist-based scoring, and uncalibrated risk models. maturity

Privacy Controls
User/device identifiers pseudonymized; analysis uses security metadata only.

Expected Outcome
Stronger auth, healthier devices, fresher telemetry → higher ZTMI and more stable trust trajectories.

olagu4@morgan.edu | onyema.osuagwu@morgan.edu