Security-per-Watt

Making Zero Trust Work When You Have Three Watts and Intermittent Comms

JONATHAN SHELBY

DPhil Computer Science Candidate | Hertford College, University of Oxford
Supervisor: Professor Andrew Martin

UK Systems Workshop 2026

THE PROBLEM

Zero Trust Assumes Abundance

NIST 800-207 ZTA requires continuous verification – but what happens when the resources to verify are fundamentally scarce?

ZTA Requires

- Continuous connectivity to policy engine
- Compute headroom for crypto operations
- Real-time trust evaluation
- Centralised policy decision point

Constrained Environments

- Intermittent or high-latency links
- Watts-level power budgets
- Minute-to-hours decision latency
- Autonomous nodes, no always-on PDP

CASE STUDY

LEO CubeSats: ZTA at the Constraint Boundary

If ZTA can work here, the framework generalises to any resource-constrained system – IoT, Edge, Tactical.

3W

Total power budget shared across all subsystems

~8 min

Ground station contact window per orbit

42

Vulnerabilities mapped STRIDE + ATT&CK + CVSS v3.1

THE FRAMEWORK

Security-per-Watt & Distributed Security

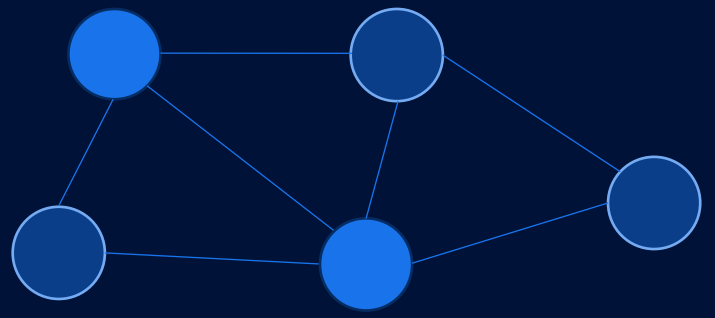
SpW = Security Posture / Power (W)

Higher SpW = more security per unit of constrained resource

- **Comparative** — Rank competing security configurations
- **Actionable** — Maps directly to engineering decisions
- **Composable** — Aggregates node → constellation posture

Distributed Security Paradigm (DSP)

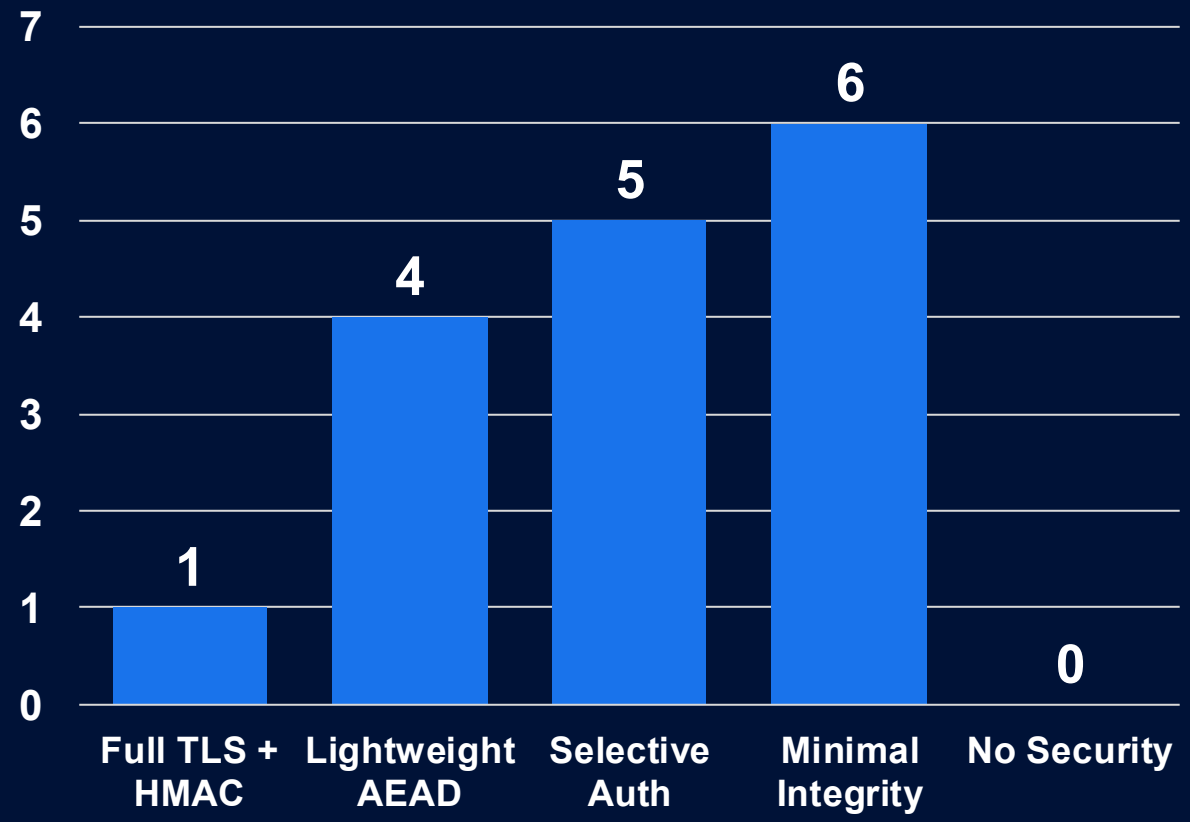
Security responsibility distributes across the constellation. No single node is the PDP – trust evaluation is autonomous and power-aware.



ZTA for constrained systems requires distributed, autonomous, power-aware trust evaluation

THE FRAMEWORK

Security-per-Watt & Distributed Security



Key findings:

- **Security is not free**
  Full enterprise ZTA is physically impossible on a 3W budget
- **The sweet spot exists**
  Selective Auth maximises security per watt consumed
- **Constellation > node**
  Distributing security functions raises aggregate SpW
- **ZTA must adapt**
  Static policy enforcement fails under intermittent communications

WHERE NEXT

From SpW to Formal ZTA Verification

SpW tells you what to deploy, One of the aspects future work seeks to prove: Can we prove this holds-up against a thinking adversary

SpR = Security Posture / Resource where Resource ∈ {Power, Bandwidth, Latency, Cost}

CSP Process Algebra

Formal behavioural specification of ZTA components with refinement verification via FDR4

Game-Theoretric Adversarial Analysis

FlipIt-style modelling of trust re-evaluation timing under strategic attack

Compositional Assurance

Do security properties proven for individual components hold when composed

Key Takeaways

- ZTA assumes resource abundance – constrained environments break that assumption
- SpW makes the security / resource trade-off explicit and quantifiable
- Distributed Security Paradigm enables ZTA without always-on connectivity
- Further research: formal verification of ZTA with CSP process algebra + game-theoretic adversarial modelling

Jonathan Shelby

Jonathan.Shelby@cs.ox.ac.uk | DPhil Computer Science Candidate, University of Oxford

Questions?