NOVAK PROTOCOL LAWS

Law L10:
Zero Trust Execution

Trust Cryptography, Not Systems

Authoritative Edition

L10 Definition

"The system must assume: data can lie, rules can drift, outputs can be corrupted, and memory can be manipulated. Only cryptography determines trust."

The Hostile Environment

NOVAK assumes the infrastructure is compromised.

Data Lies

Rules Drift

Outputs Corrupt

Memory Manipulated

The Paradigm Shift

Implicit Trust

"We are behind the firewall, so we are safe."

REJECTED

Explicit Proof

"Prove correctness for every single instruction."

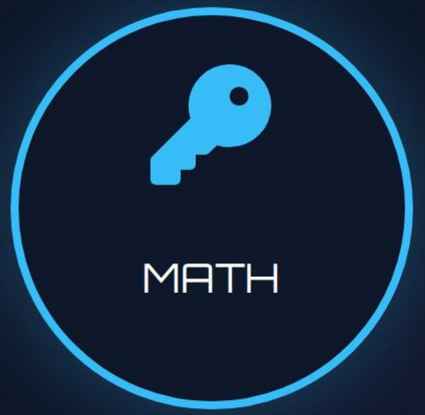
REQUIRED

No "Inside"

L10 dictates that even the kernel, the admin, and the database are untrusted actors until proven otherwise.

The Only Arbiter

If we cannot trust the admin, the network, or the hardware, what do we trust?



Cryptography is the only source of truth.

Implementation Strategy

Verify Every Step

Don't just verify the login. Verify every computation.

Assume Breach

Design as if the adversary already has root access.

Bind Everything

Use HVET/EIR to seal data against insider threats.

Impact on Government & Defense

The Insider Threat

Traditional systems fail against insiders (Snowden, Manning, Texeira). They had "access" so they were "trusted".

The NOVAK Defense

Under L10, access does not grant execution rights. Only a valid cryptographic proof allows action. An insider cannot forge the chain.

Summary

Zero
Trust

Never Trust. Always Verify.

L10 removes the concept of a "trusted user" or "safe zone". Every single action must fight for its right to exist via cryptographic proof.

Questions?

NOVAK Protocol Standards Series

Law L10: Zero Trust Execution Model