Anonymous Encrypted Relay Network

AERN Executive Summary

April 25, 2025

Overview

The Authenticated Encrypted Relay Network (AERN) represents a transformative advancement in private, anonymous, and cryptographically authenticated communications. Developed in response to the vulnerabilities of legacy anonymizing protocols like TOR, AERN establishes a fully meshed, domain-based proxy network architecture designed for high performance, post-quantum security, and complete traffic anonymization.

AERN is not a global public anonymity platform but a scalable and federated system designed for private deployment by trusted institutions. It operates on authenticated nodes, validated by a root certificate authority, using strong post-quantum cryptographic primitives and per-packet route randomization to ensure that data flows are secure, anonymous, and resistant to correlation and replay attacks.

Motivation and Problem Statement

Since its inception in the mid-1990s, TOR has offered a layered encryption system to anonymize internet traffic. However, TOR's reliance on publicly hosted volunteer nodes, its vulnerability to Sybil and traffic-correlation attacks, and its use of pre-quantum cryptography leave it exposed to both current and emerging threats. As global adversaries deploy increasingly sophisticated surveillance infrastructure and quantum computers become viable, the core design of TOR is no longer sufficient.

AERN answers this challenge with a future-proof solution that addresses these weaknesses directly. It eliminates untrusted intermediaries, ensures message integrity and confidentiality with post-quantum secure cryptography, and introduces advanced countermeasures against traffic analysis, including dynamic routing and uniform packet sizing.

Design and Architecture

AERN is built on a structured, four-tier architecture:

1. **AERN Root Security (ARS)** – Acts as the isolated trust anchor, signing device certificates and defining the cryptographic configuration set.
2. **AERN Domain Controller (ADC)** – Handles network orchestration, registration, certificate validation, topology synchronization, and revocation management.
3. **AERN Proxy Servers (APS)** – Form a full mesh of symmetric, bi-directional tunnels for relaying encrypted messages between authenticated devices.

4. **AERN Client Devices (ACD)** – Initiate secure communications through entry proxies, leveraging randomized routing to ensure anonymity.

Each proxy server exchanges asymmetric keys during network initialization, followed by symmetric key derivation for high-performance, low-latency encryption via RCS – a Rijndael-based authenticated stream cipher. Proxy communication occurs over dynamically generated circuit paths with a randomized number of hops (default range: 3–16), refreshed on a per-packet basis.

Key Features

- **Quantum Resistance**: Employs NIST-selected post-quantum primitives – Kyber, McEliece, Dilithium, SPHINCS+ – for all asymmetric operations.
- **Symmetric Tunnel Mesh**: After initialization, all communications rely solely on symmetric cryptography, enabling thousands of low-latency, encrypted tunnels.
- **Fixed-Size Packets**: Every packet is 1500 bytes (standard MTU), eliminating traffic fingerprinting via size analysis.
- **Route Randomization**: Circuit paths change with every packet, severely hampering timing and flow-correlation attacks.
- **Replay Protection**: Packet headers include UTC timestamps and sequence numbers; expired or duplicated messages are dropped and connections torn down.
- **Zero Metadata Retention**: AERN servers do not log packet data or metadata. All session state is ephemeral and erased upon termination or timeout.
- **Scalable Domain Deployment**: Supports multiple federated AERN domains, allowing operators to offer AERN instances as VPN alternatives.

Security and Anonymity Strengths

- **Authenticated Entry and Exit**: Every node is authorized via ARS-signed certificates, eliminating risks from malicious volunteers or rogue nodes.
- **Traffic Obfuscation**: Uniform packet size, randomized routes, and per-hop symmetric re-encryption effectively defeat deep-packet inspection and correlation.
- **Administrative Isolation**: The root server is offline or air-gapped, with only proxy-signing functionality enabled through the ADC, supporting hardened deployment environments.
- **Post-Quantum Assurance**: All cryptographic primitives are resilient to both classical and quantum adversaries, exceeding current TOR capabilities.

Applications and Deployment Scenarios

AERN is ideal for:

- **Governments and Defense**: Secure classified communications across national proxy domains.
- **Enterprises and FinTech**: Anonymous encrypted tunnels for sensitive transactions and internal operations.

- **Human Rights and Journalism**: Trusted infrastructure for secure reporting and anonymous information exchange.
- **Critical Infrastructure**: Scalable, authenticated, low-overhead encrypted communications for SCADA, IoT, and emergency systems.

Conclusion

AERN presents a paradigm shift in secure and anonymous communication, abandoning the weaknesses of public anonymizers in favor of a verifiable, domain-controlled infrastructure. By fusing robust post-quantum cryptography with scalable and efficient tunneling mechanisms, AERN is poised to become the successor to legacy anonymity networks. Its design is ready for standardization, enterprise adoption, and future-proof security deployments in a post-quantum world.