NovaKey Threat Model (High-Level)

System Overview

NovaKey is a local, device-to-device secure input system consisting of an iOS application and a desktop daemon. The threat model focuses on protecting user input in transit between trusted devices while acknowledging out-of-scope threats.

Primary Assets

- User keystrokes and clipboard contents (in transit only)
- Session encryption keys
- Paired device trust records

Adversaries Considered

- Network attackers (passive and active MITM)
- Replay attackers attempting to reuse captured traffic
- Unauthorized devices attempting to inject input

Threats & Mitigations

Network interception: Mitigated by XChaCha20-Poly1305 authenticated encryption.
Future quantum decryption: Mitigated by ML-KEM-768 during session establishment.
Replay attacks: Mitigated by per-device nonce cache and freshness checks.
Unauthorized injection: Mitigated by pairing allowlist, policy gates, and optional two-man approval.

Explicit Non-Goals

NovaKey does not attempt to protect against a fully compromised host OS, malicious kernel drivers, or physical access attacks. These are explicitly out of scope.