

Hermes

A practical SPARTA-LL Implementation

Surendra Jammishetti

Mar 16, 2025

CSE 108C

Problem Defenition

- Current anonymous messaging systems aren't resilient to traffic analysis attacks.
- SPARTA lays a framework for a fast, traffic analysis resistant solution.
- Common pitfalls, such as user validation, that can starve user messages.
- Lacks details for multi-device communication.

Threat Model and Security Guarantees

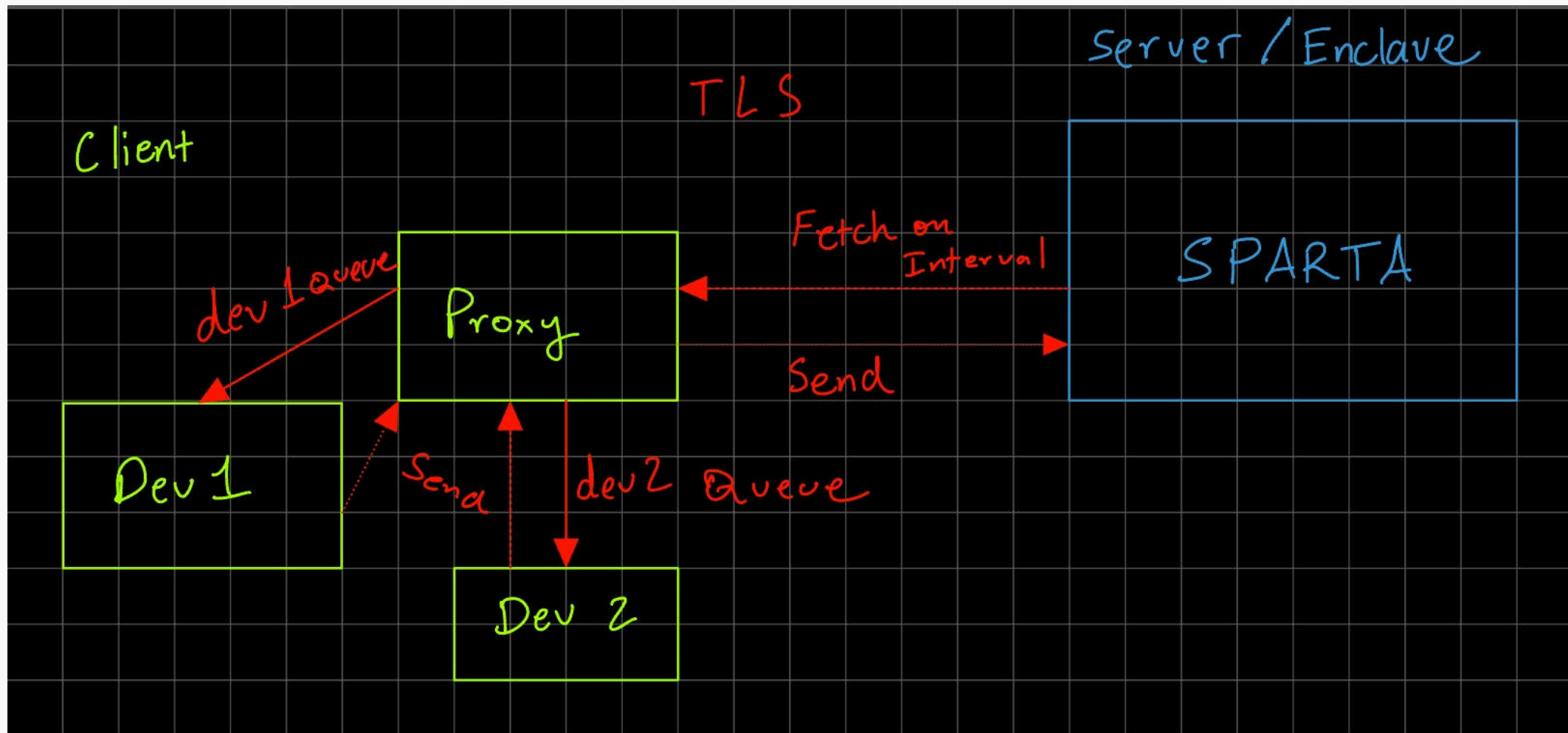
Adversary

- Inheriting SPARTA's threat model of a global active attacker who can
 - control / modify all network links
 - participate in the protocol
 - observe traffic for an arbitrary amount of time
 - can breach everything on the server excluding the enclave code

Differential Privacy

- Guarantee that adversary cannot correlate that one user is messaging another.
 - The base SPARTA-LL construction already achieves this.

My Approach



Implementation Details

- No enclave (lack of hardware)
- 2.5k lines of rust
- GRPC as messaging protocol
- Facebook ORAM Implementation
- $O(N \log(N))$ Implementation for UserStore OMAP
- ed25519 Signatures to determine Fetch authenticity
- Proxy has queue per device to hold older messages

Results

