INCHEON NATIONAL UNIVERSITY

CYBERSECURITY CONVERGENCE LAB

CAMEO

: Callback-Aware Mediation and Enforcement Overlay

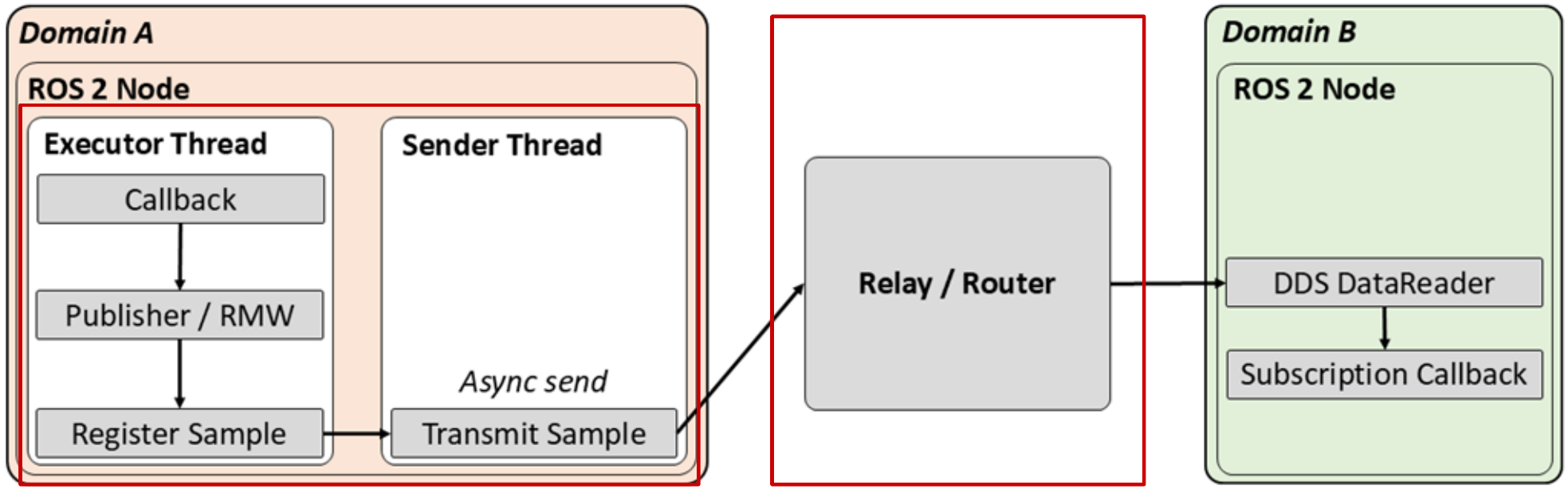
Yunseo Choi, Seungsoo Lee

Department of Computer Science & Engineering

Incheon National University

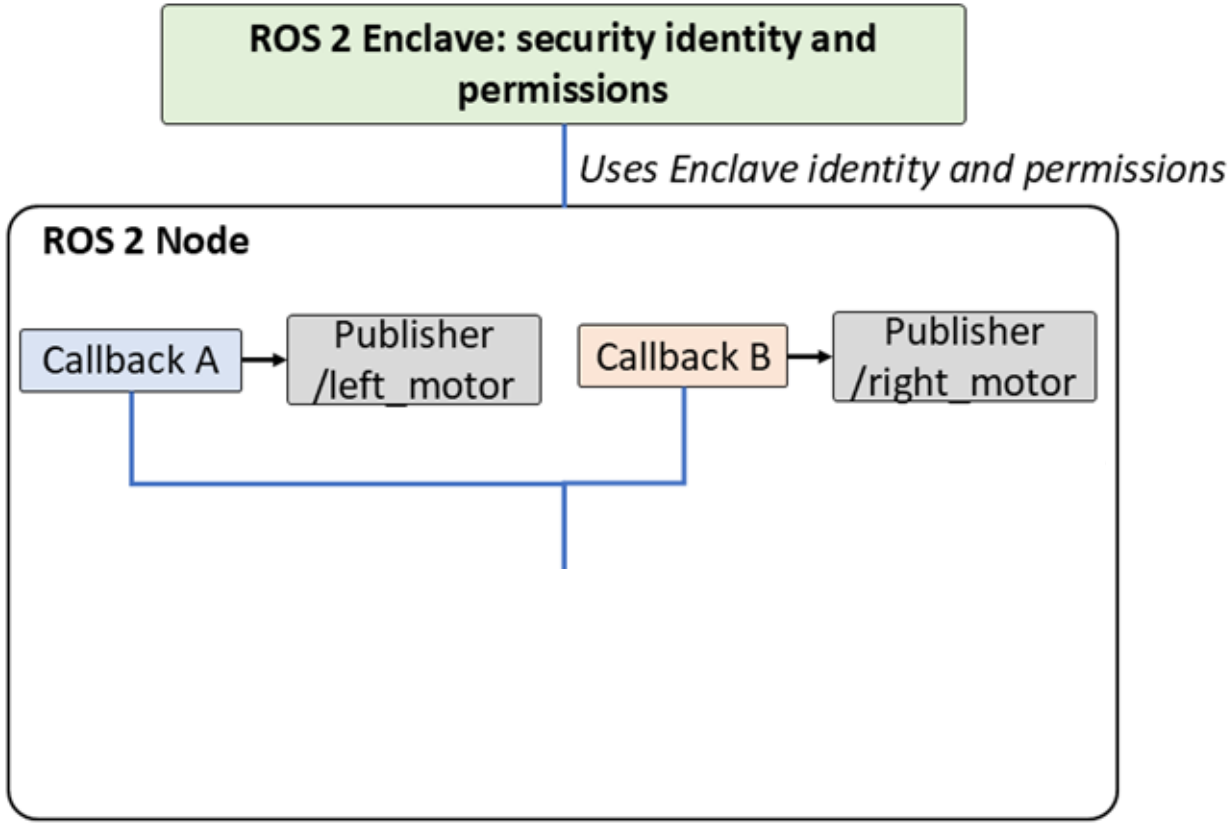
Background [1] ROS 2 and DDS Communication

- Robot Operating System 2(ROS 2) publication → Data Distribution Service(DDS) Sample
- Cross-Domain communication through routers or relays
- Fast DDS asynchronous publication: separate Callback execution and Sample transmission threads



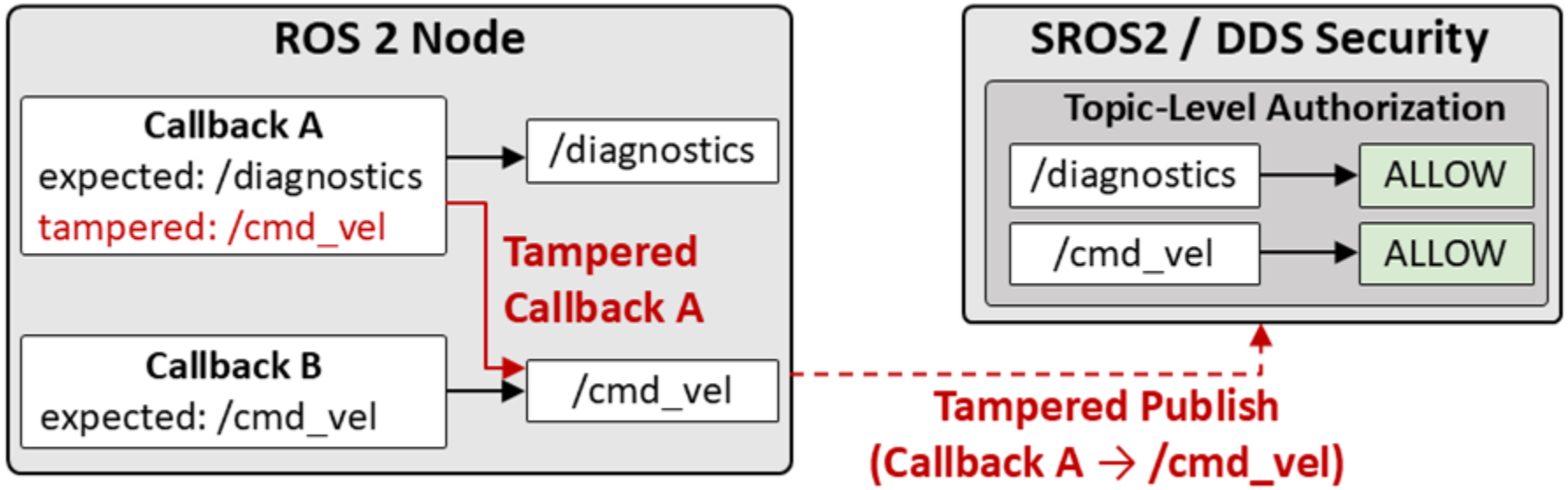
Background [2] SROS2 and DDS Security

- Enclave-based DDS Security identities and permissions
- Participant authentication and Topic-level access control
- Shared security context across Callbacks within a Node



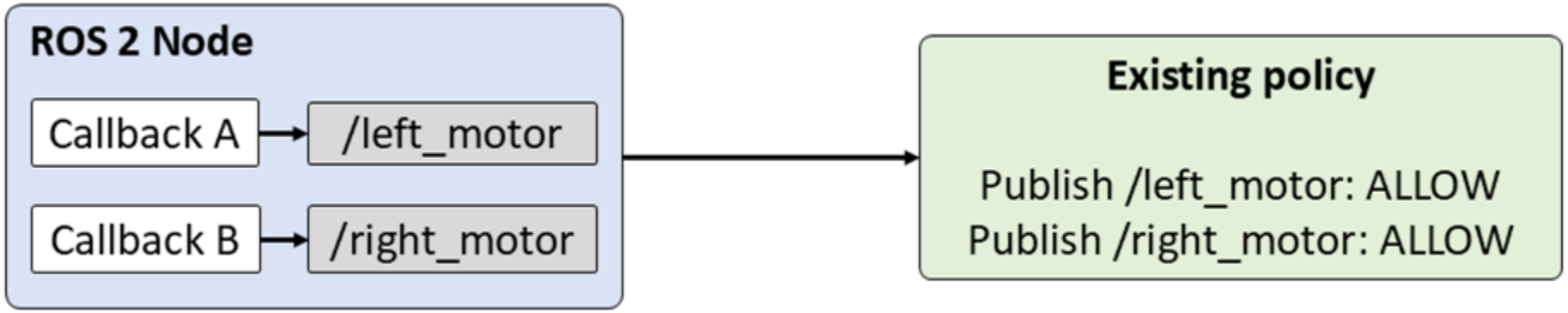
Problem Statement [1] Lack of Callback-Level Cross-Domain Authorization

- Node/Participant-level permissions without originating Callback identification
- No Callback-level authorization for Cross-Domain delivery



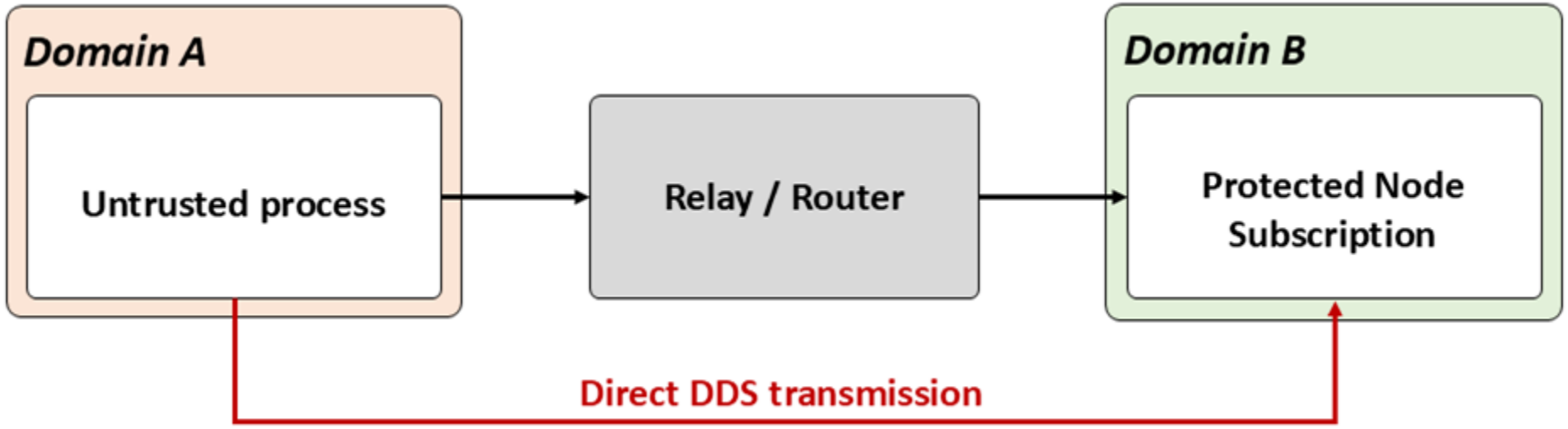
Problem Statement [2] Lack of Callback-Level Least-Privilege Policies

- Existing policy generation based on Node–Topic relationships
- No per-Callback output Topic distinction

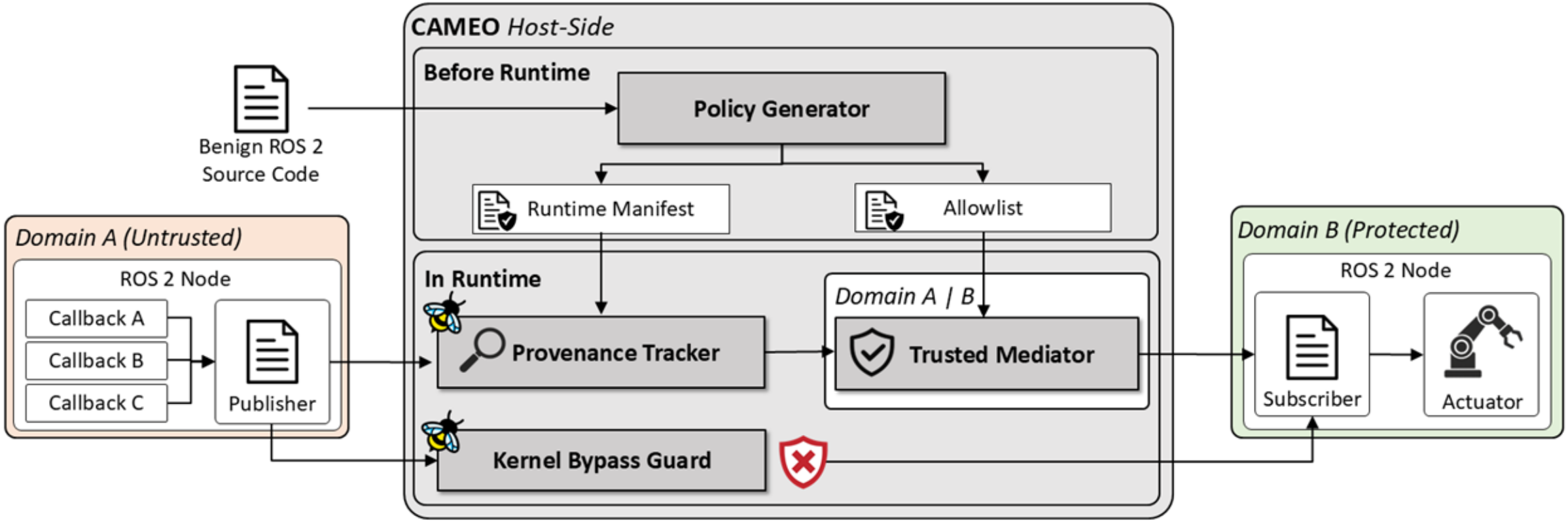


Problem Statement [3] Bypass of the Protected-Domain Mediation Path

- Direct DDS transmission to the protected Domain
- Bypass of the mediation path and Callback-level authorization

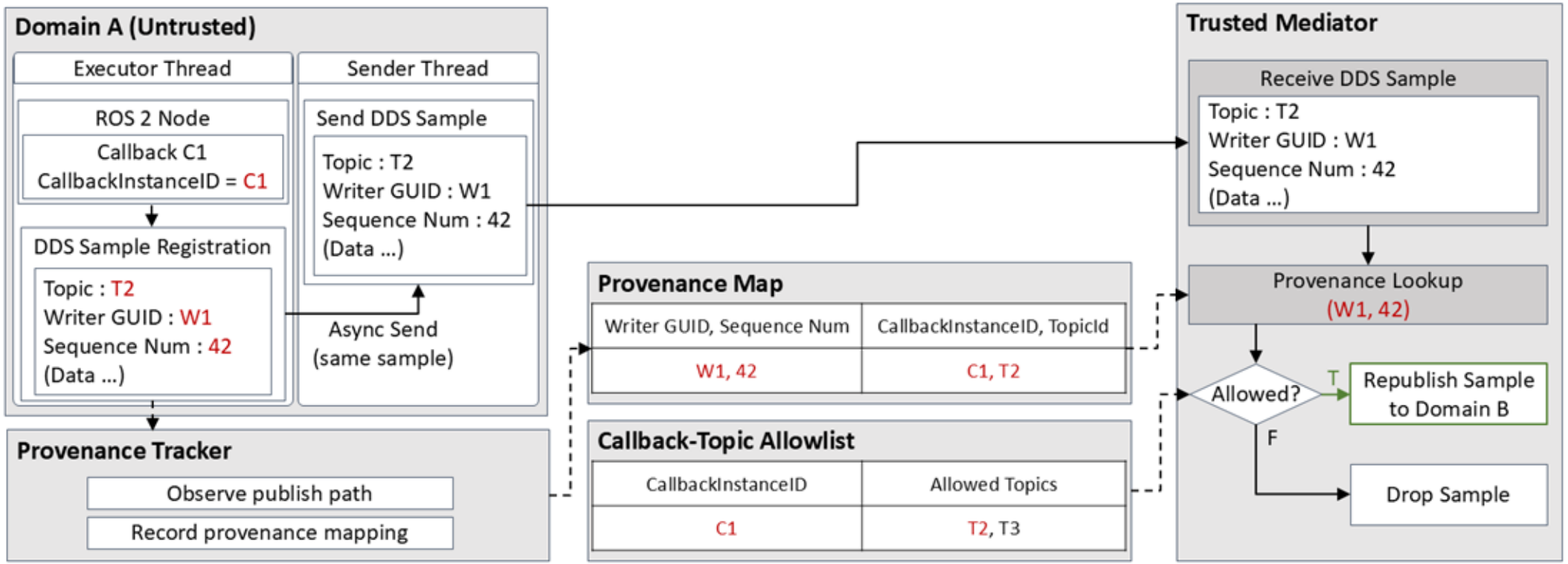


Overall Architecture



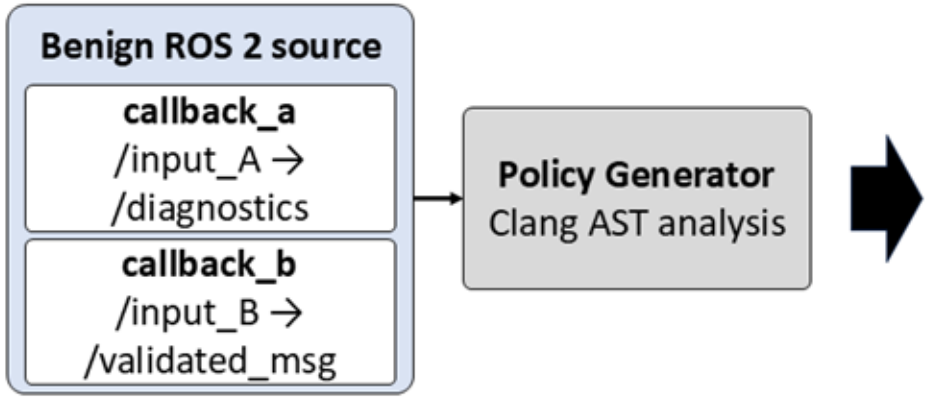
System Design [1] Callback-Level Authorization

- DDS Sample–Callback provenance mapping
- Callback–Topic Allowlist enforcement at the Trusted Mediator



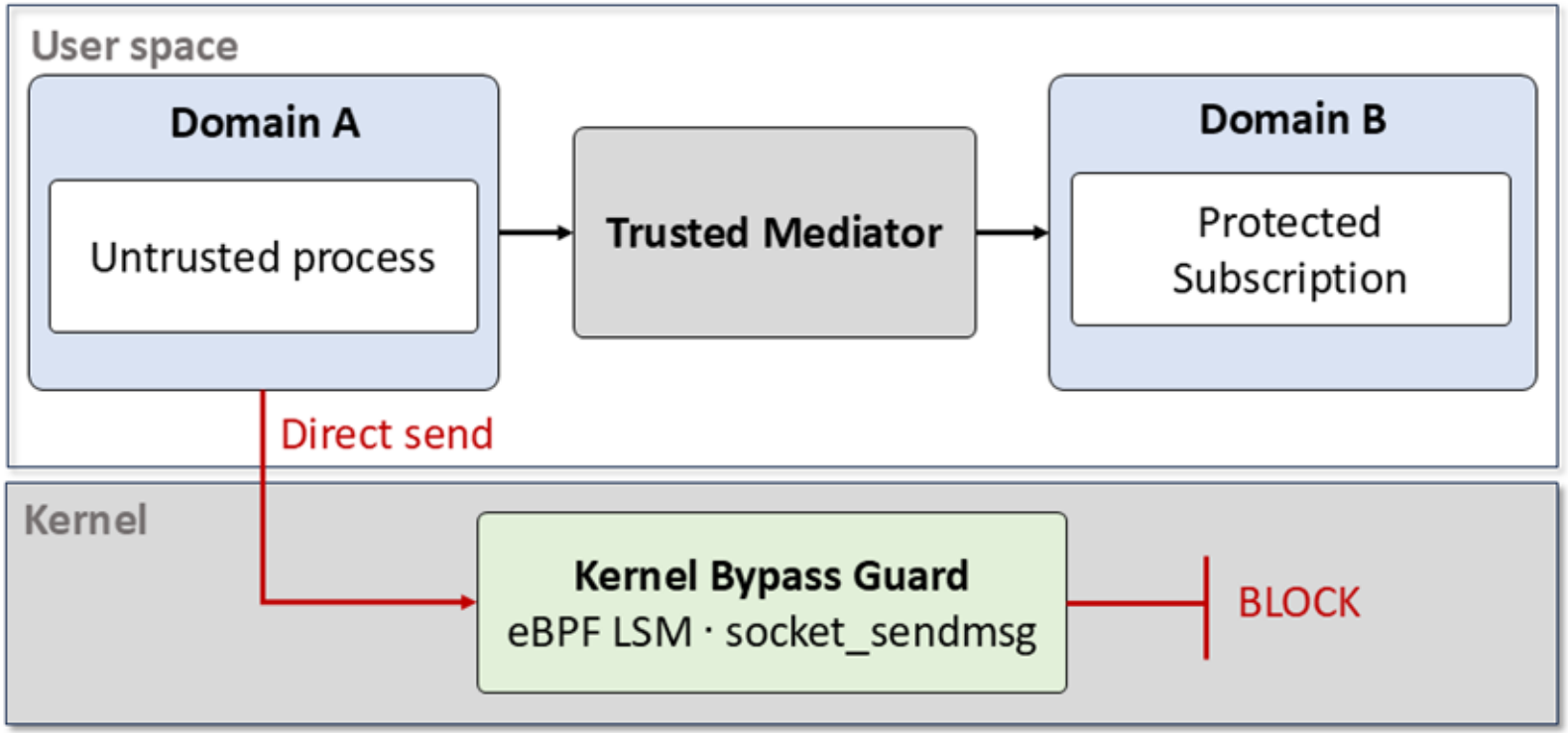
System Design [2] Callback-Level Least-Privilege Policy Generation

- Clang AST-based extraction of benign Callback–Topic relationships
- Runtime Manifest and Callback–Topic Allowlist generation



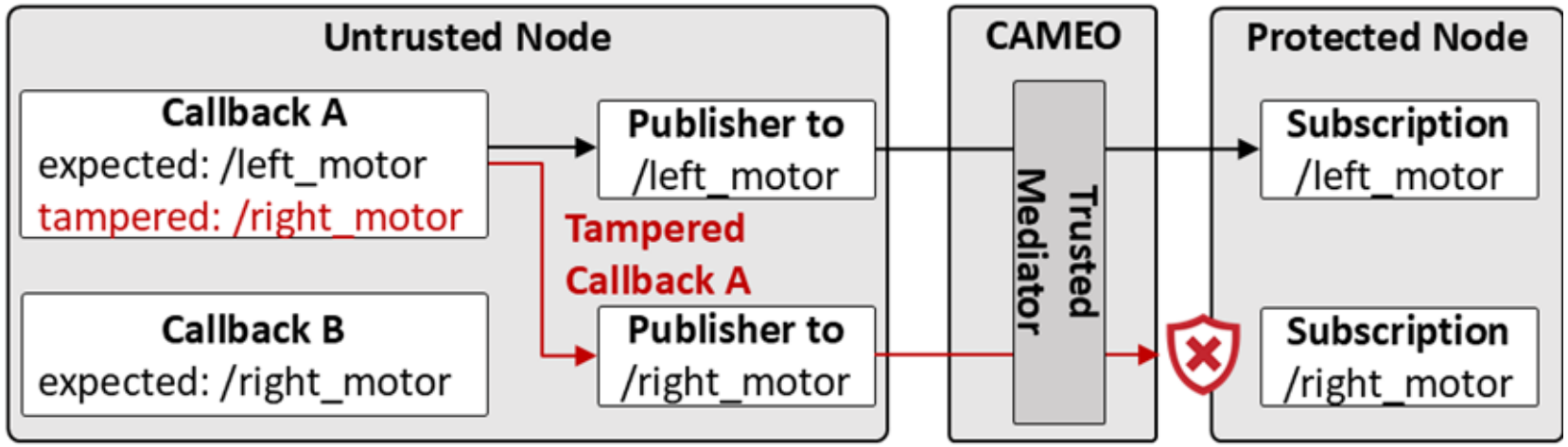
System Design [3] Blocking Direct Transmissions to the Protected Domain

- extended Berkeley Packet Filter(eBPF) Linux Security Module(LSM) enforcement at `socket_sendmsg`
- Direct protected-Domain transmission blocking for registered untrusted processes
- Scope: Fast DDS IPv4 UDP



Evaluation [1] Callback-Level Authorization

- CAMEO: authorized delivery preserved; Callback privilege abuse blocked
- SROS2: privilege abuse permitted under shared Topic permissions

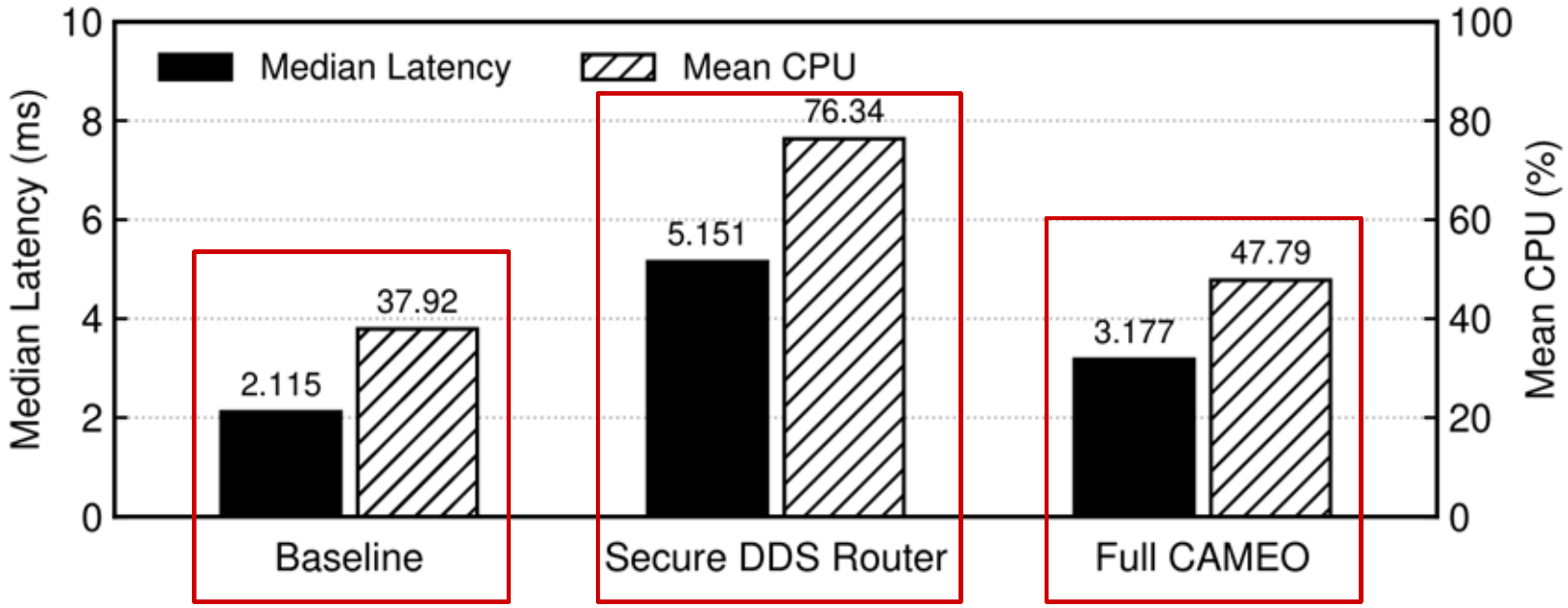


Evaluation [2] Policy Generation and Bypass Prevention

- Generated Allowlists: exact Ground Truth match
- Direct transmission blocking: 0/300 without Guard → 300/300 with Guard

Evaluation [3] Cross-Domain Performance

- vs. Baseline: median latency **+50.2%**, mean CPU usage **+26.0%**
- vs. Secure DDS Router: median latency **−38.3%**, mean CPU usage **−37.4%**



Conclusion

- **Fine-Grained Authorization**
  - Originating Callback identification and per-Callback Cross-Domain authorization
- **Automated Least-Privilege Policy Generation**
  - Source-derived Callback-Topic Allowlists
- **Mandatory Mediation**
  - Kernel-enforced prevention of direct protected-Domain transmissions

Q&A