

Path Validation Application Scenarios

Side Meeting on Path Validation

D. López (*Telefónica*)

IETF#118, Prague (Czech Republic), November 2023

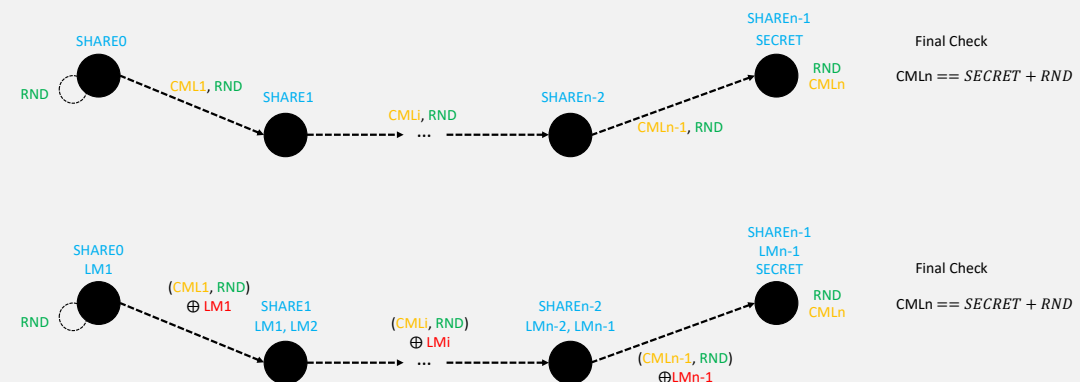
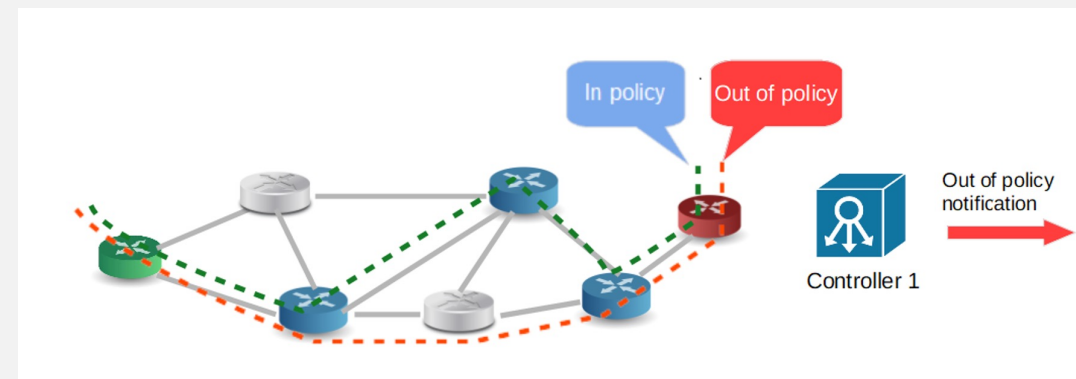
Verifiability as a Must

- The Software Network is here
 - Not any longer a future trend
 - NFV, SDN, disaggregation, Open-RAN, microservices...
- The cloud as a common model
 - Challenging all current trust and security assumptions
 - New models for deployment, collaboration, assurance, accounting...
- And the network invariants
 - Topology (and geometry!) awareness
 - The conservation principle
 - Openness
 - Integrity and auditability
 - Isolation



The Basic Use Case Topology Attestation

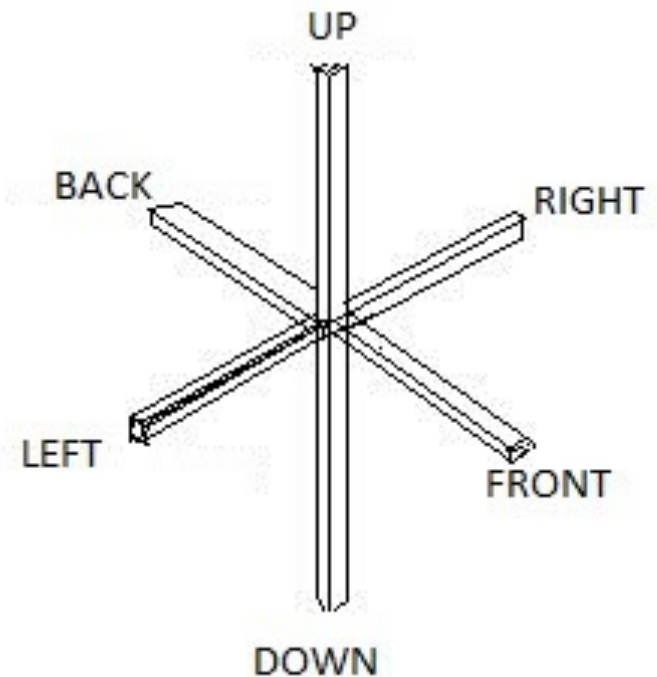
- Via Proof of Transit
 - Effective attestation at the data plane
- Prove traffic goes through specific elements
 - Packets and flows
 - According to a policy
 - Verifiable by third parties
- Add extra metadata to packets
 - Provide crypto to prove transit
 - Be careful with the obvious penalties



Application Scenarios

Security Policy Enforcement

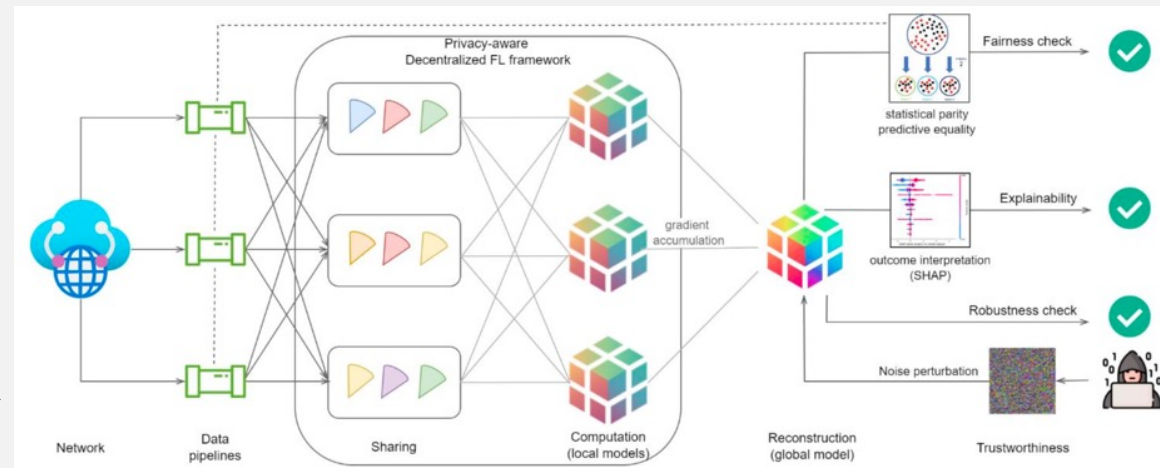
- Customers select specific security functions
 - By orchestration (NFV, SDN...) or policy (a-la-I2NSF)
 - The service provider produces sequential evidence of applying these functions
- Customers require traffic to follow a specific secure overlay/underlay
 - Secured links
 - Trusted execution environments
 - Non-repudiation
 - Even in a per-packet basis, if required...



Application Scenarios

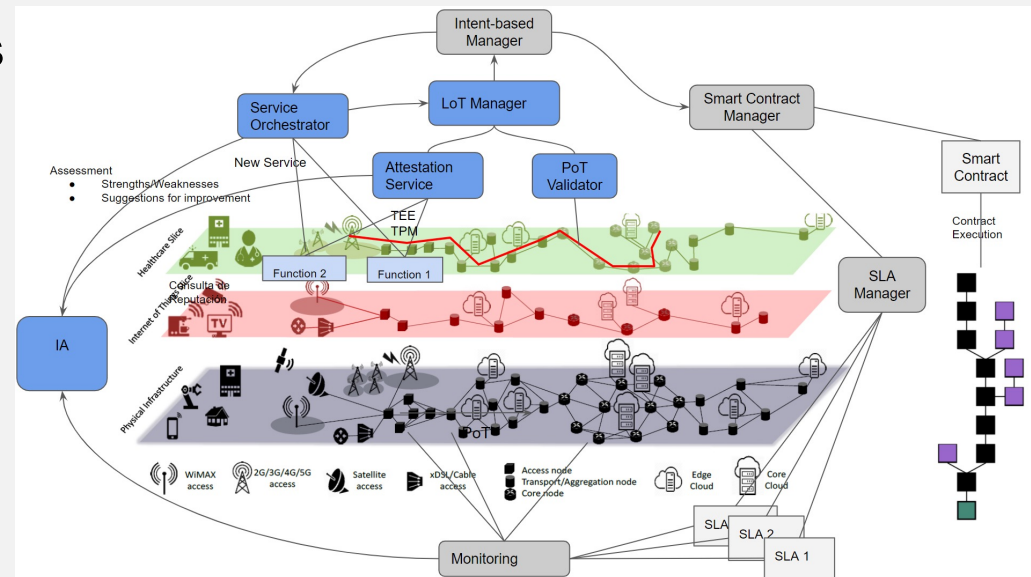
Routing Compliance

- Geofencing
 - Verify customer data remains within defined geolocations, such as their campus or native country.
- Verify path properties
 - Specific implementations
 - Infrastructure providers
 - Not properly update devices
 - Privacy preserving functions
 - . . .
- Support trustworthy telemetry
 - As collected by reliable nodes
 - Requested measurements along the path



Application Scenarios Evaluating Level of Trust

- Level of Trust
 - Assess the trustworthiness of a network service in a particular application environment
 - Combine security and privacy aspects
- Integrate objective and subjective inputs
 - Crypto in use
 - Platform and software attestations
 - Supply chain
 - Reputation
 - Proof-of-transit
 - . . .
- Associated with service levels
 - Verifiable by third parties
 - Suitable for smart contracts
 - Support for intent



What We Are Interested in

- Current PoT is performed applying secret sharing schemas
 - Each element holds the share of a secret
 - Provided by a controller
 - Applied to metadata
 - Verified at the end of the network function chain being attested
- Willing to explore new mechanisms to achieve it
 - Reduce penalties
 - Extend applicability
 - Consider the combination with other Path Validation approaches