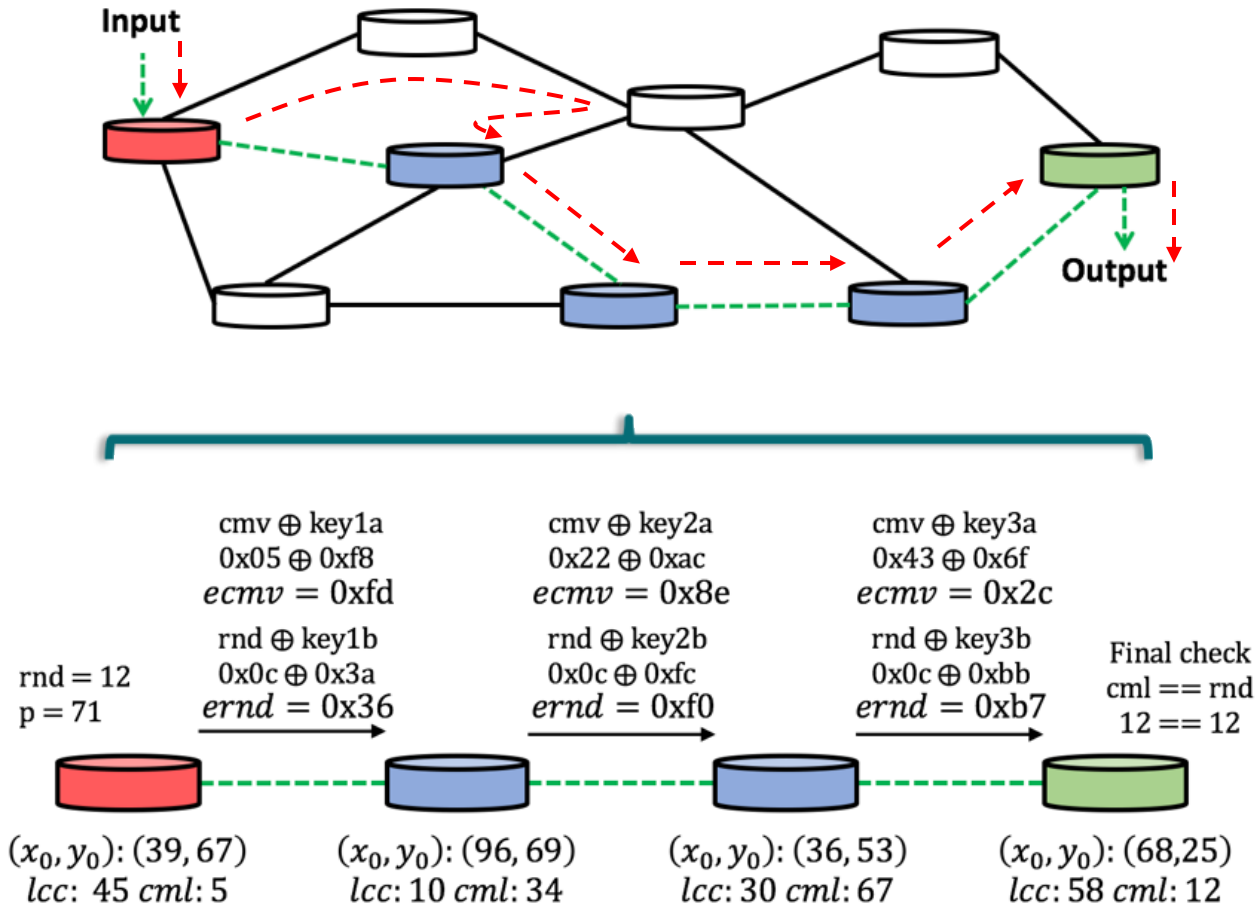
A Proposal to the NASR Cabal on PoT and TPR Convergence

A. Pastor, **D. López** (*Telefónica)*

NASR Side Meeting @ IETF#119, Brisbane (AU), March 2024

Proof of Transit (draft-ietf-sfc-proof-of-transit-08)



Proof of Transit (PoT)

Also in PoT Option-Type in IoAM (RFC 9197)

Pro:

- E2E per packet (or sampled) path verification to a subset of nodes in a domain
- Can use any encapsulation (UDP, NSH, IPv6, IoAM)
- Integrity protection possible (draft-ietf-ippm-ioam-data-integrity-07)
- Can verifiy the order with symmetric mask
  - Ordered PoT (OPoT) Sec.3.5 in draft-ietf-sfc-proof-of-transit-08

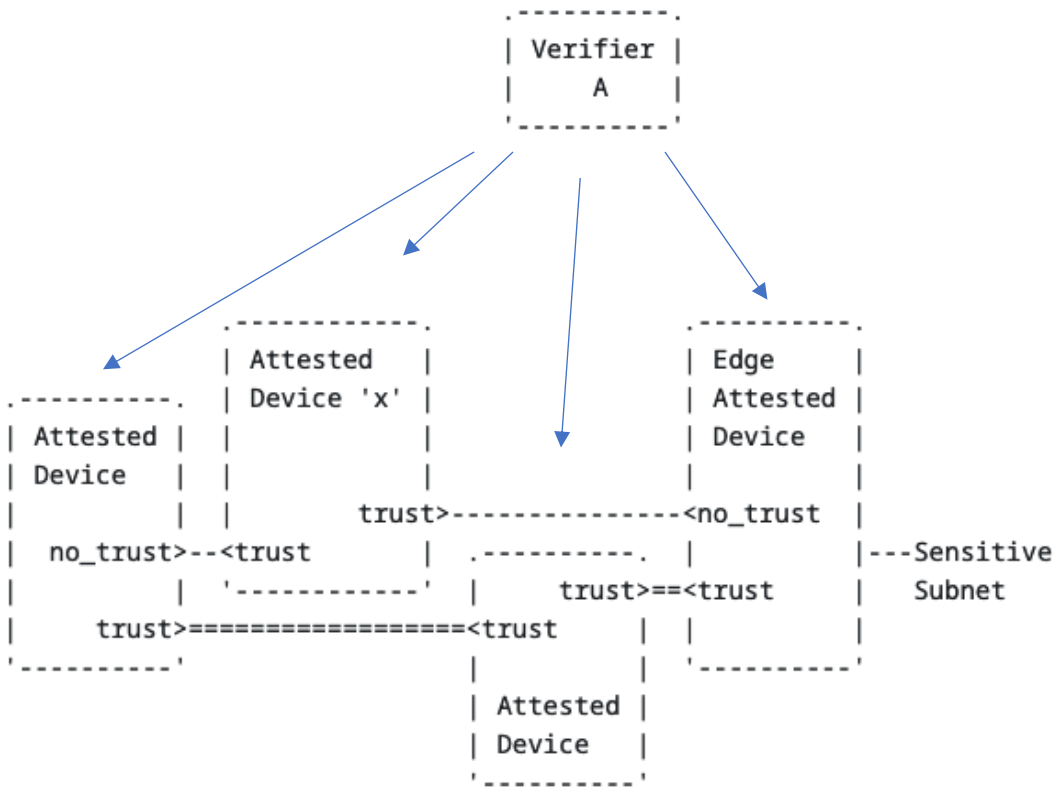
Cons:

- No protection against additional nodes in the path
- MiTM
- PonT

trustworthy-path-routing (draft-voit-rats-trustworthy-path-routing-09)

Trusted Path Routing (TPR)
Mutual attestation of nodes (routers) through L2 links
Pro:
- List of attested nodes & interfaces (integrity verification from boot)
- Apply only to selected IP subnets

Cons:
- Changes in the path must be detected by other means
- No protection outside the sensitive subnets
  - Multi-domain issues



The Proposal: A(ssured)PoT = TPR + PoT

- ALL devices have PoT functionality (e.g. IoAM PoT)
- TPR verifiers share the information of each device and link list (trusted topology) with the PoT controller
- The PoT controller calculates the exact path to follow
  - Identifying the specific nodes in the sensitive subnet
  - And distributes the crypto material accordingly to the nodes, related to TPR results
- Pro:
  - Traffic integrity in nodes is provided by TPR and the *PoTted* path
  - TPR guarantees the integrity of the PoT Software (not altered or disabled)
  - ALL nodes in the sensitive network have PoT, so if traffic goes through an extra node PoT verification will fail
- Cons:
  - Still multi-domain issues
  - What goes outside a sensitive subnet

Two More to Explore: AOPoT and Interdomain

- AOPoT, integrating OPoT
  - Derive masks for Ordered PoT from TPR creation results in each direction of the traffic
  - Periodic appraisal will renew masks
- Interdomain validation
  - Exchange of material to support E2E path validation and protection
  - TPR: *Golden values* across domains by verifiers
    - Considerations on privacy and network information exposure
  - PoT: E2E SSS schema (plus inter-domain masks)
    - Architectural and trust issues