Path Validation Scenarios
Build and Verify

A. Pastor, D. López (Telefónica)

NASR BoF @ IETF#120, Vancouver, July 2024
The Ingredients for Path Validation

• Means for assessing specific properties on a particular network path
  • Whatever their nature, generally related to a security posture
  • Geolocation
  • Versioning / patch level
  • Supported features
  • ...

• Attestation of the path components
  • When constructing the path
  • Relaying on RATS

• Attestation of the path behavior
  • During its use
  • Relaying on PoT
Path Construction

• Trustworthy Path Routing (TPR)
  • draft-voit-rats-trustworthy-path-routing
• Mutual attestation of nodes (routers) through L2 links

• List of attested nodes & interfaces
  • Integrity verification from boot
• Apply only to selected IP subnets

• Changes in the path not detected
  • Other means required
• No protection outside the sensitive subnets
• Multi-domain issues
Path Behavior

- **Proof of Transit**
  - `draft-ietf-sfc-proof-of-transit`
  - PoT Option-Type in IoAM (RFC 9197)

- **E2E per-packet/sampled path verification**
  - For a subset of nodes in a domain
  - Use any encapsulation: UDP, NSH, IPv6, IoAM
  - Integrity protection possible
    - `draft-ietf-ippm-ioam-data-integrity-07`

- **Order verification based on symmetric masks**
  - Ordered PoT (OPoT)
    - Sec.3.5 in `draft-ietf-sfc-proof-of-transit-08`

- **No protection against additional nodes in the path**
  - MiTM
  - PonT
The Recipe: 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
• Traffic integrity in nodes is provided by TPR and the PoT ted 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

• Still multi-domain issues
• What goes outside a sensitive subnet
Two More Aspects to Explore Order and Interdomain

• AOPoT, integrating OPoT
  • Derive masks for Ordered PoT from TPR creation results in each direction of the traffic
  • Periodic assessment 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