IETF 121 – IETF

Network Attestation for Secure Routing (NASR)

Luigi Iannone

Material presented in these slides is based on NASR BoF @ IETF 120

IETF 121 – Dublin

Pointers and historical information on NASR

- Current NASR description (https://datatracker.ietf.org/doc/bofreq-liu-nasr/)

- NASR Formal non-WG forming BoF held at IETF 120:
  - https://datatracker.ietf.org/group/nasr/meetings/
- NASR Side Meeting at IETF 119:
  - https://github.com/liuchunchi/nasr_side_meeting
- Path Validation Side Meeting at IETF 118:
  - https://github.com/liuchunchi/nasr_side_meeting/tree/main/IETF%20118%20Path%20Validation%20Side%20Meeting%20Archive
- Internet Drafts
  - NASR Use Case and Requirements:
    - draft-liu-nasr-requirements-03: https://datatracker.ietf.org/doc/draft-liu-nasr-requirements/
  - Terminology and Use cases for Secured Routing Infrastructure
    - draft-richardson-nasr-terminology-01: https://datatracker.ietf.org/doc/draft-richardson-nasr-terminology/
  - Network Attestation for Secure Routing (NASR) Architecture
    - draft-liu-nasr-architecture-01: https://datatracker.ietf.org/doc/draft-liu-nasr-architecture/

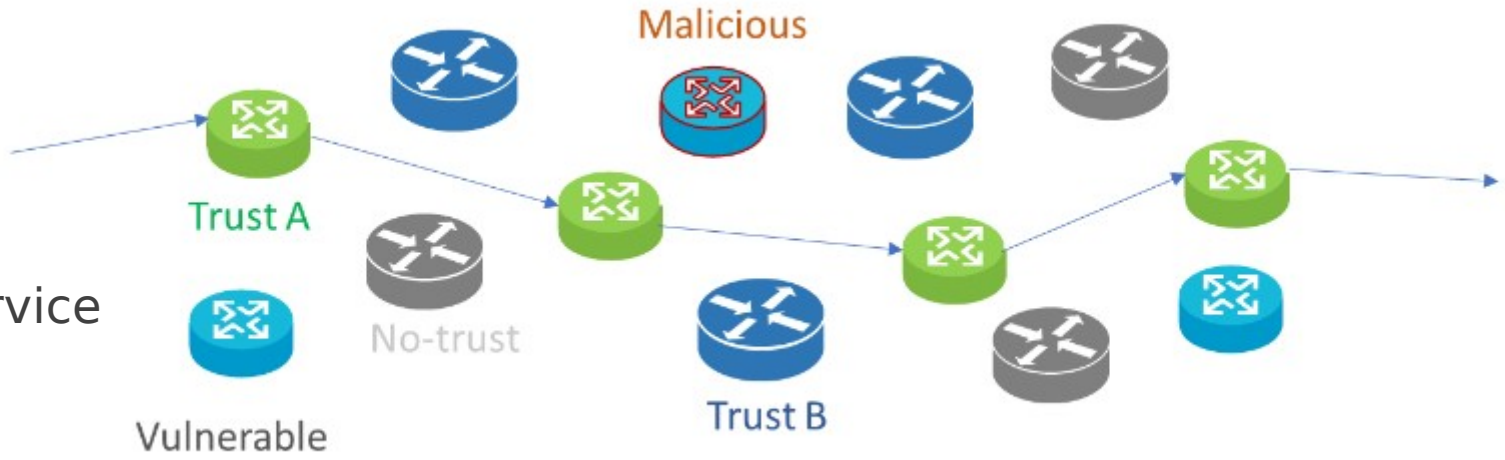
The problem

- The data, plain or encrypted, if accessed by insecure/untrusted devices, could be copied, cryptanalyzed for decryption or forgery; or dropped.

- How to achieve dependable hop-by-hop forwarding on top of trusted devices and links only, so to minimize data leakage/exposure to insecure/untrusted devices.

- Integrity-checked device that executes forwarding dependably minimizing risks

- Major Use cases:
  - SFC Proof of Transit
  - SLA Auditing
  - Enterprise Trusted Connection service
  - Data sovereignty



What about VPNs/TLS/IPSec ??

- **No perception to the path and network elements trustworthiness, so traffic can be accessed and processed by insecure devices, permitting further attacks**

- **Crypto-exploit**
  - Store-Now, Decrypt Later attacks (Quantum computer attack)
  - Deprecated/Unsecure cryptography
  - Known implementation issues

- **Data exposure**
  - VPNs implies a privileged middlebox (encryption is not end-to-end but segment-to-segment)

- **Lack of audit tools**
  - Impossibility to verify path and network element trustworthiness
  - Impossibility to very packet transit

NASR main objectives

- Clients with **high security and privacy requirements are not anymore satisfied with pure encryption-based data security measures in the application or transport layer that do not allow any control over the underlay networks. Clients now require their data to exclusively traverse the network through trusted devices, trusted operating environments, trusted links and trusted services**, avoiding any exposure to insecure or untrusted devices. Hence, how to establish routing trustworthiness and transparency so as to achieve predictable forwarding behaviors becomes the main challenge.
- **The goal** of Network Attestation for Secure Routing WG is to **address the challenges associated with** routing data on top **of trusted devices, trusted operating environments, trusted links and trusted services** only, so as **to achieve transparent and predictable forwarding behavior**. Verifiable operational correctness proofs should also be given to serve as a trusted evidence for visualization, internal inspection and external auditing.

- **Forwarding Path Auditing**
  - Prove traffic **went through specific elements (Proof of Transit)**
  - Prove traffic **went through elements with certain properties (Trustworthiness)**

Why this Presentation?

- **Excerpt from: https://datatracker.ietf.org/rg/panrg/about/**

  - Increased diversity in access networks, and ubiquitous mobile connectivity, have made this architecture's assumptions about paths less tenable. Multipath. protocols taking advantage of this mobile connectivity begin to show us a way forward, though: **if endpoints cannot control the path, at least they can determine the properties of the path by choosing among paths available to them.**

- **NASR is a specific instantiation of the above-mentioned problem, enabling to choose among paths via auditing and can verify if the selected path has been followed!**

LIDE TO BE USED IN PANRG

- **Feedback from this group really appreacited**

THANKS!

LIDE TO BE USED IN PANRG

Why this Presentation?

- **Comments during the BoF @ IETF 120 and discussion on the mailing list pointing to NASR and ANIMA complementary depending on use case**

- Excerpt from: https://datatracker.ietf.org/wg/anima/about/

  - The Autonomic Networking Integrated Model and Approach (ANIMA) working group develops and maintains specifications and documentation for interoperable protocols and procedures for automated network management and control of professionally-managed networks.

- **NASR has different, narrower, objective specific to auditing forwarding paths and collect & verify proof of transit.**

LIDE TO BE USED IN ANIMA WG

- **Feedback from this group really appreacited**

- Points of discussion
  - Automating NASR with ANIMA?
  - Can NASR leverage on RFC 8995 Bootstrapping Remote Secure Key Infrastructure (BRSKI)?
  - Can NASR leverage on RFC 8994 An Autonomic Control Plane (ACP)?
  - Trust Model?

THANKS!

LIDE TO BE USED IN ANIMA WG