

18 March 2024

IETF 122 NASR

Network Attestation for Secured foRwarding

Problem Statement and Proposed Architecture

- Peter (Chunchi) Liu, Michael Richardson

Why NASR: what solution we are looking for, to enable these use cases?

AS-IS:

Problem 1:

- Customers cannot control which **geolocation** the traffic transit

Problem 2:

- Customers cannot request traffic traverse devices, links, services that **meet their certain security requirements**
 - Integrity-checked, latest patched, use certain crypto...

Result:

- **Encrypted traffic could be captured** + traffic pattern analysis/ endpoint key leak/ capture-now-decrypt-later / middlebox inspection/ = **sensitive information leak**

Current Solution AS-IS:

- Customers **implicitly trust** the connection the operator provides, with no control, visibility or confidence.
- Operators have **no means to provide assurance** to such service properties.

TO-BE

- Customer traffic only traverse compliant devices within **certain geolocations**.

- Customer traffic only traverse compliant devices with **certain security attributes, minimize security posture**
 - Cannot guarantee 100% no compromise – but can guarantee you use state-of-the-art patches, best crypto...

Result:

- **No traffic detour**, thus no leakage (even encrypted)
- **No vulnerable/old devices**, thus no leakage (even encrypted)
- **No vulnerable links**, thus no leakage (even encrypted)

Solution TO-BE:

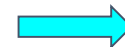
- Customers have **visibility and verifiability** to his security requirements.
- Operators **assure path behavior and path security components, provide verifiable proofs** to customers.

Why NASR now?

- **Attestation technology (e.g., RATS) provides foundations to assess and visualize device security**
- **NASR now drives attestation technology to go further**

1. Attestation technology is **ready** in various vendor' s core products.
 - Development of NASR on top of RATS' work is tractable.
2. Attestation technology allows stricter security assumptions such as **accountable forwarding**, thus **assured network behavior**.
 - Close the gap between **routing security VS forwarding security**.
3. Attestation technology allows **security distinction** to network devices, thus **security-enhanced connectivity**.

○ **Choose** preferred devices, **setup** path and **verify** forwarding.



What is NASR?

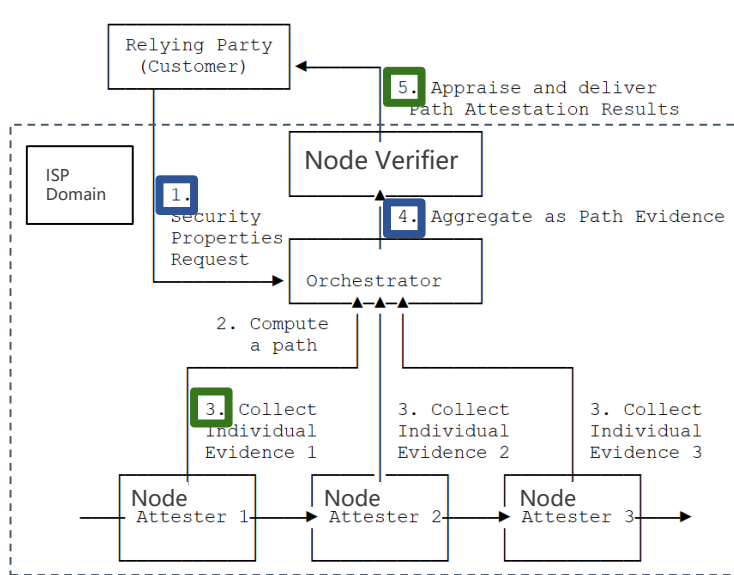
What is NASR: Architecture at-a-glimpse

Solution Steps:

Choose → Setup → Verify

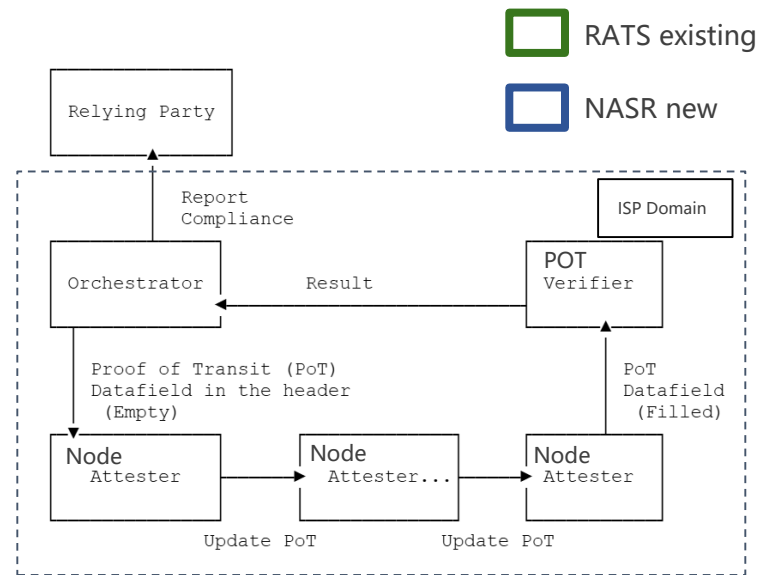
[“Prepare/Choose”] Clients choose a set of security properties he desires for a network deployment, Orchestrator compute a path

1. [“Before use/Setup”] Orchestrator collect attesters/devices properties on this path (via YANG/BGP-LS), attest to them, create **baseline**.
2. [“During use/Verify”] Continuously **verify** the forwarding behavior against the **baseline** (e.g., through Proof of Transit, data plane ext.).



Step 1: Service Path Attestation
(YANG example)
(When Prepare and Before Use)

Similar to measured boot!
Simplest POT is compute iterative hash at link



Step 2: Proof Of Transit
(when service in actual use)

THANKS!