25 July 2024

IETF 120 NASR (BoF)

Network Attestation for Secure Routing

This session is being recorded

Internet Engineering Task Force

Production by Meetecho

IETF

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/ (Privacy Policy)

To Be Updated When IETF 122 Agenda Available

IETF

Note Really Well

- IETF meetings, virtual meetings, and mailing lists are intended for professional collaboration and networking, as defined in the IETF Guidelines for Conduct (RFC 7154), the IETF Anti-Harassment Policy, and the IETF Anti-Harassment Procedures (RFC 7776). If you have any concerns about observed behavior, please talk to the Ombudsteam, who are available if you need confidentiality to raise concerns confident about harassment or other conduct in the IETF.
- The IETF strives to create and maintain an environment in which people of many different backgrounds and identities are treated with dignity, decency, and respect. Those who participate in the IETF are expected to behave according to professional standards and demonstrate appropriate workplace behavior.
- IETF participants must not engage in harassment while at IETF meetings, virtual meetings, social events, or on mailing lists. Harassment is unwelcome hostile or intimidating behavior—in particular, speech or behavior that is aggressive or intimidates.
- If you believe you have been harassed, notice that someone else is being harassed, or have any other concerns, you are encouraged to raise your concern in confidence with one of the Ombudspersons.

To Be Updated When IETF 122 Agenda Available

IETF

This session is being recorded

IETF 120 Meeting Tips

To Be Updated When IETF 122 Agenda Available

In-person participants

- Make sure to sign into the session via Datatracker or the QR Code in this session.
- Use Meetecho (usually the "Meetecho lite") client to:
  - join the mic queue
  - participate in shows of hands
- *Keep audio and video off if not using the onsite version.*

Remote participants

- Make sure your audio and video are off unless you are chairing or presenting during a session.
- Use of a headset is strongly recommended.

Resources for IETF 120 Vancouver

- Agenda & Slides:
  - https://datatracker.ietf.org/meeting/120/session/nasr
- Notepad:
  - https://notes.ietf.org/notes-ietf-120-nasr
- Zulip Room:
  - https://zulip.ietf.org/#narrow/stream/nasr
- Audio Stream:
  - https://mp3.conf.meetecho.com/ietf120/33219.m3u
- Meetecho
  - Remote Stream: https://meetings.conf.meetecho.com/ietf120/?session=33219
  - Onsite Tool: https://meetings.conf.meetecho.com/onsite120/?session=33219

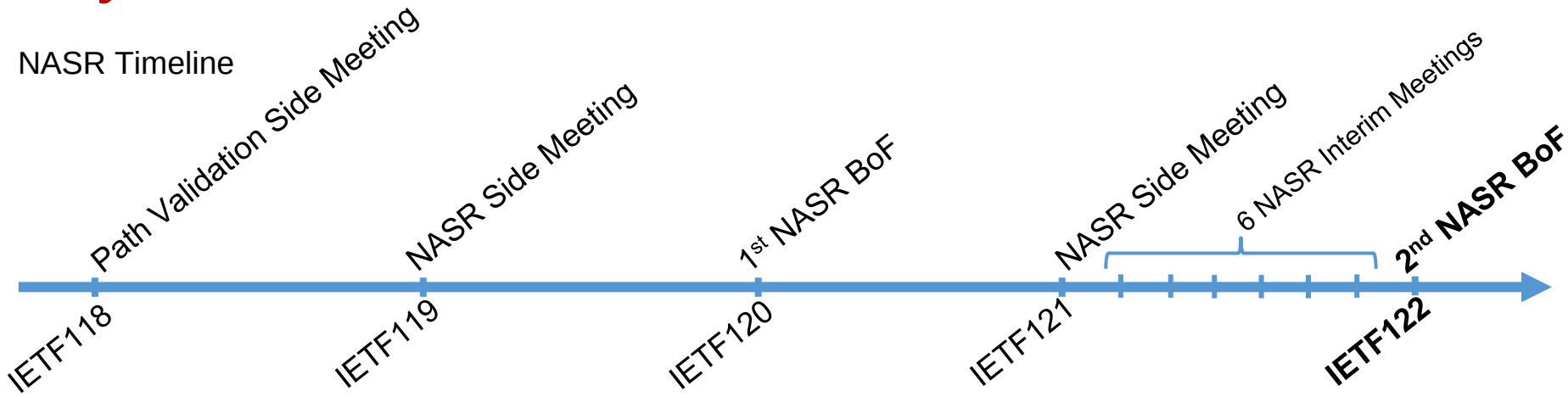
Agenda

- Note Well and Agenda Bashing - Chairs
  - 5 Minutes
- Why are we here? - Chairs
  - 5 Minutes
- Use Case & Problem Statement – MCR??
  - Use Cases (Lac Leman Example)
  - Problem Formulation
    - 35 Minutes
- Charter Discussion – Chairs
  - Summary feedback previous BoF and how concerns have been addressed
  - Proposed Charter Overview
    - 30 Minutes
- Open Mic - Feedback from the community
  - 25 Minutes
- Explore Consensus & Next Steps – Chairs & AD
  - 20 Minutes

Agenda – Why are we here?

- Note Well and Agenda Bashing - Chairs
  - 5 Minutes
- **Why are we here? - Chairs**
  - **5 Minutes**
- Use Case & Problem Statement – MCR??
  - Use Cases (Lac Leman Example)
  - Problem Formulation
    - 35 Minutes
- Charter Discussion – Chairs
  - Summary feedback previous BoF and how concerns have been addressed
  - Proposed Charter Overview
    - 30 Minutes
- Open Mic - Feedback from the community
  - 25 Minutes
- Explore Consensus & Next Steps – Chairs & AD
  - 20 Minutes

Why are we here?



BoF Goals

- The aim of this BoF is to determine – "if a WG with the proposed charter can be formed?"
  - Scope is clear?
  - Deliverables are clear?
  - Critical mass of contributors?

Agenda

- Note Well and Agenda Bashing - Chairs
  - 5 Minutes
- Why are we here? - Chairs
  - 5 Minutes
- **Use Case & Problem Statement – MCR??**
  - **Use Cases (Lac Leman Example)**
  - **Problem Formulation**
    - **35 Minutes**
- Charter Discussion – Chairs
  - Summary feedback previous BoF and how concerns have been addressed
  - Proposed Charter Overview
    - 30 Minutes
- Open Mic - Feedback from the community
  - 25 Minutes
- Explore Consensus & Next Steps – Chairs & AD
  - 20 Minutes

Technical Presentation

1. Clients can choose a set of ("trusted") properties,
2. these properties are verified on a path through attestation,
3. the behavior can be audited and (repeatedly) verified (e.g., Proof of Transit).

Agenda

- Note Well and Agenda Bashing - Chairs
  - 5 Minutes
- Why are we here? - Chairs
  - 5 Minutes
- Use Case & Problem Statement – MCR??
  - Use Cases (Lac Leman Example)
  - Problem Formulation
    - 35 Minutes
- **Charter Discussion – Chairs**
  - **Summary feedback previous BoF and how concerns have been addressed**
  - **Proposed Charter Overview**
    - **30 Minutes**
- Open Mic - Feedback from the community
  - 25 Minutes
- Explore Consensus & Next Steps – Chairs & AD
  - 20 Minutes

1st BoF Feedback Summary & Proposed Changes

- **From IAB:**
  - *The BOF's name includes "secure routing", which also contributed to some confusion since the focus is on *forwarding*, not routing.*
    - Changed acronym meaning:
      - Old: NASR – Network Attestation for Secure Routing
      - New: NASR – Network (remote) Attestation for Secured foRwarding
    - Clarified scope from routing to forwarding (see proposed charter)
  - *…due to the broad nature of the use cases and the liberal use of terminology, there were also many clarifying questions.*
    - Work on to describing a specific use case succinctly (technical presentation)
      - Also added as work item (see proposed charter)
    - Simplified and unified terminology
      - Work item (see proposed charter)

1st BoF Feedback Summary & Proposed Changes

- **From IAB:**
  - *Discussing the NASR scenarios in PANRG may help the proponents clarify the terminology and focus the use cases before a second BOF.*
    - Luigi Iannone presented @ PANRG IETF 121
      - Feedback during meeting on already identified concerns:
        - Routing vs Forwarding
          - Corollary: PoT can be used *"standalone"* in other scenarios
        - Proof of Non-transit
    - Clarified scope from routing to forwarding (see proposed charter)
    - Added threat analysis task (see proposed charter)
      - Informal feedback after PANRG meeting showed support and interest
  - *SCION has addressed some of the scenarios and needs (except for PoT)*
    - The group is in contact with SCION authors which also are regular attendees of NASR meetings

1st BoF Feedback Summary & Proposed Changes

- **From Community (during 1st Bof and/or mailing list):**
  - *What does "Secure Routing" stand for in NASR?*
    - See similar point raised by IAB and at PANRG
    - Clarified scope from routing to forwarding (see Proposed Charter)
  - *Mixed and unclear usage of terms "secure" and "trust"* NASR does not target large scale deployment in the open Internet.
    - See similar point raised by IAB, the variety of presented use cases had a different use of these terms.
    - Simplified and unified terminology
      - Work item (see proposed charter)

1st BoF Feedback Summary & Proposed Changes

- **From Community (during 1st Bof and/or mailing list):**
  - *What is the relation/overlap with SAVNET WG?*
    - SAVNET Chairs and NASR Chairs discussed a text stating SAVNET and NASR are complementary (presented at the 1st BoF)
      - SAVNET goal is to provide a mechanism to determine valid incoming router interfaces for specific source prefixes. NASR aims at providing secure routing via mechanisms to make packets follow a trusted path.
    - Other WG discussed proposed charter
  - *What is the relation with the IAB Statement about the risks of attestation on the open Internet*
    - https://datatracker.ietf.org/doc/statement-iab-statement-on-the-risks-of-attestation-of-software-and-hardware-on-the-open-internet/
    - NASR does not target large scale deployment in the open Internet.
    - NASR aims at providing a technical solution for services that have intentionally specific requirements concerning path devices attributes and provable transit.

Proposed Charter – Motivation & Background

- In the current network deployments, **communicating entities** implicitly rely on peer entities and use paths as determined by the control plane. These **available path(s) are implicitly trusted**. Communicating entities have very little information about the entities in the paths over which their traffic is carried, and have no available means to audit the entities and paths, beyond basic properties like latency, throughput, and congestion. However, **increased demand in network security, privacy, and robustness makes tools for enabling visibility of the entities' security posture a necessity.**
- Path-agnostic traffic signing and encryption has been the primary method to ensure data confidentiality, integrity and authenticity today. However, with the increasing amount of attacks, and vulnerabilities, new emerging threats are imposing requirements that go beyond the data security currently provided. Vulnerable factors include:
  - Exploitation of poor cryptographic engineering
  - Side-channel attacks
  - Untrusted network devices (e.g., middlebox decryption and/or inspection)
  - Unauthorized data duplication (capture now decrypt later)
  - Unauthorized device root access, caused by physical tampering or penetration
  - Erroneous routing to unintended devices or areas, etc.
- With these additional security and privacy requirements, there is a **need to provide enhanced or added services beyond the pure encryption-based data security**; **requiring better visibility of the security posture of the underlying network elements.** Specifically, to satisfy the visibility of the network elements' security state, proof that data is traversed through network elements (devices, links and services) that satisfy security posture claims to avoid exposure of unqualified elements is needed.
- The **RATS (Remote ATtestation procedureS) working group** has provided a framework and approaches to assess and establish the trustworthiness of a single device, hence offering an **initial building block.** However, a comprehensive framework that attests to a network -- meaning **network-level elements' trustworthiness proofs and verification methods are lacking.**

Proposed Charter - Goals

1. The Network Attestation for Secured FoRwarding working group **is (being) chartered to address the challenges associated with proving state and characteristics of a network path are compliant to a set of claims, so as to achieve predictable and verifiable forwarding behavior**. The work will build as much as possible on existing standards and implementations, focusing on combining them in a clear and coherent manner to address secured forwarding use cases such as those identified and described in the NASR use cases and requirements document.

1. The working group will **initially focus on** a simple source-routing path in **limited domains** [RFC8799] under a single administrative control. The working group **will then focus on** a path spanning **a few numbers of limited domains that have business relationship**, in order to help coordinate, connect and deliver a consistent connectivity service. Applying NASR to large groups of domains such as the Internet is not seen as viable and useful use case.

Proposed Charter - Scope

- **In Scope**
  - Architecture and procedures of network path attestation
  - Interface among limited number of domains having business relationships
  - Proof-of-Transit mechanisms to verify forwarding path in the data plane

- **Out of Scope**
  - Path computation according to a set of claims.
  - Automated operational security incident remediation, routing fault correction.
  - Methods of how to assess device integrity and/or trust-level.
  - Public Internet deployment.
  - Proof of non-transit.

Proposed Charter – Key Deliverables

- **NASR Use Cases, Problem Statement and Requirements:**
  - A description of use cases, formalize their requirements and the problem to be solved, including a threat analysis.
- **NASR Architecture:**
  - An architecture that defines the interactive procedures of network path attestation, along with definitions of common terminology, roles, trust models etc.
- **NASR Service Model:**
  - A definition of the standard service interface between operators and operator clients, translate client requests to objective security features or trust attributes, making sure the same service request will receive same security levels services from different operators.
- **NASR Path Attestation Claims Set:**
  - Attested claims set that describes state and characteristics of a network path comprised of network elements. It should be collectively defined by all network elements in the path, and encoded in certain encapsulation formats. This claims set is used by a relying party, to determine if the operator delivers the requested security requirements.
- **NASR Proof of Transit:**
  - Mechanisms and protocol extensions for Proof-of-Transit (PoT), proving and visualizing the actual forwarding paths in the data plane.

Proposed Charter - Relation with Other WGs

- The NASR working group will coordinate and collaborate with other WGs as needed. Specific expected interactions include (but may not be limited to):
  - RATS on the remote attestation technology.
  - PANRG on path-aware networking aspects.
  - Other IETF WGs and IRTF RGs that address topics related to attestation, routing security, like for instance SAVNET, SIDROPS.

Agenda

- Note Well and Agenda Bashing - Chairs
  - 5 Minutes
- Why are we here? - Chairs
  - 5 Minutes
- Use Case & Problem Statement – MCR??
  - Use Cases (Lac Leman Example)
  - Problem Formulation
    - 35 Minutes
- Charter Discussion – Chairs
  - Summary feedback previous BoF and how concerns have been addressed
  - Proposed Charter Overview
    - 30 Minutes
- **Open Mic - Feedback from the community**
  - **25 Minutes**
- Explore Consensus & Next Steps – Chairs & AD
  - 20 Minutes

Open Mic

- Please scan QR code to login to Meetecho and join the queue …

Agenda

- Note Well and Agenda Bashing - Chairs
  - 5 Minutes
- Why are we here? - Chairs
  - 5 Minutes
- Use Case & Problem Statement – MCR??
  - Use Cases (Lac Leman Example)
  - Problem Formulation
    - 35 Minutes
- Charter Discussion – Chairs
  - Summary feedback previous BoF and how concerns have been addressed
  - Proposed Charter Overview
    - 30 Minutes
- Open Mic - Feedback from the community
  - 25 Minutes
- **Explore Consensus & Next Steps – Chairs & AD**
  - **20 Minutes**

Wrap-Up Questions

- Please scan QR code to login to Meetecho and be ready to respond to the upcoming polls…

Naming Choices

1. NASR: Network Attestation for Secured foRwarding (changed from Secure Routing)
   - Emphasize “what we want to achieve”

1. FELPA: Forwarding Evidence by Local and Path Attestation
   - Emphasize “how we want to do it”

Wrap-Up Questions (may be separated on several slides…)

1. **Is the problem well understood?**

1. **Is this problem tractable?**

1. **Is the IETF the right place to address the problem?**

1. **Is there support to form a WG with the proposed charter?**
    - Assuming that any further charter revision proposal will be discussed and made

Next Steps

THANKS!