25 July 2024

IETF 120 NASR (BoF)

Network Attestation for Secure Routing

This session is being recorded

Internet Engineering Task Force

Production by Meetecho

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)

I E T F®

Note Really Well

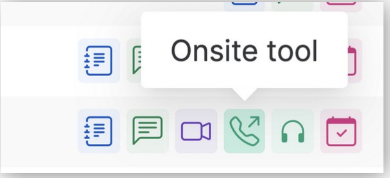
- IETF meetings, virtual meetings, and mailing lists are intended for professional collaboration and networking, as defined in the IETF Guidelines for Conduct (RFC 7154), the IETF Anti-Harassment Policy, and the IETF Anti-Harassment Procedures (RFC 7776). If you have any concerns about observed behavior, 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.

This session is being recorded

IETF 120 Meeting Tips

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

Resources for IETF 120 Vancouver

- Agenda
  https://datatracker.ietf.org/meeting/agenda
- Meetecho and other information:
  https://www.ietf.org/how/meetings/preparation
- If you need technical assistance, see the Reporting Issues page:
  http://www.ietf.org/how/meetings/issues/

Agenda Bashing

- 5min Agenda bash – notetakers?
- 5min Why are we here? - Chairs
- Use cases, Business, and Technology drivers
  - 10min Secure Routing Path Considerations - Meiling Chen
  - 10min Path Validation Application Scenarios - Diego Lopez
  - 10min Path Characteristics Verification and Attestation Services - Yutaka Oiwa
  - 10min Trusted connection service for enterprise customers with high security requirements - Yu Fu
  - 10min End-to-end use cases (AI and beyond) which require NASR - Ramki Krishnan
  - 5min Use Case Consolidation for NASR - Liu Chunchi (Peter)
- 10min Problem Statement - Liu Chunchi (Peter)
- 15min Proposed initial Architecture - Michael Richardson
- 20min Open Mic / Discussion
- 10min Next Steps - Chairs

Why are we here?

NASR BoF was previously discussed as **NASR Side Meeting at IETF 119 and Path Validation Side Meeting at IETF 118.**

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

- **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.

Is it covered by other WGs/RGs? (I)

- RATS
  - RATS (Remote Attestation Procedures) working group has provided **a framework and approaches to assess and establish the trustworthiness of a single device**. Several individual submissions are also offering part of the solution to achieve NASR goal. However, **a comprehensive framework that allows network/path trust appraisal, attestation, trust-aware routing or packet steering, and provide verifiable proof of forwarding, remains elusive**.*

- SAVNET
  - **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.** Also providing evidence that packets indeed went through the expected trusted path. While SAVNET depends on correct routing announcements, NASR can be used to detect unexpected routing behavior. The deployment model is also different. Intra-domain SAVNET focuses on validating traffic that comes from other ASes, Customers, or hosts. To work, NASR has to be deployed along the whole path so to assess trust and provide proof of transit. As such they can work together in scenarios where the source of the packets is outside the domain where NASR and SAVNET are deployed, with SAVNET validating incoming packets and NASR routing them in a secure fashion.**

*Excerpt from: https://datatracker.ietf.org/doc/bofreq-liu-nasr/

** Text produced with SAVNET WG Chairs

Is it covered by other WGs/RGs (II)

- PANRG
  - 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 endpoints a mechanism to make packets follow a trusted path.**
  - Synch with PANRG chairs pending

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

Technical Presentations

Wrap-Up Questions

1. Is the problem well understood?

2. Is this problem tractable?

3. Is the IETF the right place to address the problem?