08 January 2024

NASR Interim Side Meeting
Network AtteStation for accountable foRwarding

⚠ **This Session is Recorded**

Agenda

1. Nancy & Luigi: Meeting opening
   - ○ Any Comment on last meeting minutes?

2. Overview existing Pull Requests on Charter: All
   - ○ https://github.com/ietf-nasr/NASR-Charter

3. New Name for the group: All

If time allows:

1. NASR Service Model: Meiling Chen
2. RATS Conceptual Message Wrappers (CMW) in NASR: Henk Birkholz

Any Comment on last meeting minutes?

- Minutes/Material/Recording available at:
  - https://github.com/ietf-nasr/NASR-Meetings/tree/main/NASR-Interim-11-Dec-2024

Charter: Background and Motivation introduction updated

● **Before: Background and Motivation**

Traffic signing and encryption has been insofar the primary method to ensure data confidentiality, integrity and authenticity. However, an increasing amount of attacks, vulnerabilities, and new emerging requirements are deeming the data security provided by device-agnostic signing and encryption methods insufficient. Vulnerable factors include:

● **Now: Background and Motivation**

In the Internet architecture, communicating entities blindly trust and use paths as determined by the control plane. These available path(s) are assumed to be usable, trustable, performant, and realizing the expected requirements. Communicating entities have very little information about the paths over which their traffic is carried, and have no available means to audit paths, beyond basic properties like latency, throughput, and congestion. However, increased demand in network security, privacy, robustness, and confidentiality makes tools for path properties accountability a necessity.

Path-agnostic traffic signing and encryption has been insofar the primary method to ensure data confidentiality, integrity and authenticity. However, an increasing amount of attacks, vulnerabilities, and new emerging requirements are deeming the data security provided by such methods insufficient. Vulnerable factors include:

Charter: Background and Motivation proposed changes

Customers with high security, privacy, and resiliency requirements are not any more satisfied with simple end-to-end encryption-based security measures, which does not allow assessing security and trustworthiness aspects of the underlying network elements. Emerging customers' demands include proofs that data traverse through network elements (devices, links and services) satisfying specific requirements, avoiding any exposure to unqualifying elements. Customers would like to propose path requirements, such as paths composed of devices with the latest security updates, have passed integrity checks, or routes confined within specific geographical areas. Accordingly, operators should provide verifiable proofs to the customers for operational visualization, internal inspection and external auditing.

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 remains elusive.

○ **See next slide for the diff from current version**

~~Clients~~**Customers** with high ~~security~~**security, privacy,** and ~~privacy~~**resiliency** requirements are not ~~anymore~~**any more** satisfied with ~~pure~~**simple** end-to-end encryption-based ~~data~~ security measures, ~~having no confidence of the~~**which does not allow assessing** security **and trustworthiness** aspects of the underlying network elements. ~~Clients now require~~**Emerging customers' demands include** proofs that data traverse through ~~security-satisfying~~ network elements (devices, links and ~~services),~~**services) satisfying specific requirements,** avoiding any exposure to unqualifying elements. ~~Clients~~**Customers** would like to propose ~~security~~**path** requirements, such as paths composed of devices with the latest security updates, have passed integrity checks, or routes confined within specific geographical areas. Accordingly, operators should provide verifiable proofs to the ~~clients~~**customers** for operational visualization, internal inspection and external auditing.

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~~**device, hence** offering ~~part of the solution to achieve NASR goal.~~**an initial building block.** However, a comprehensive framework that attests to a ~~network--~~**network --** meaning network-level ~~security~~**elements' trustworthiness** proofs and verification methods remains elusive.

New Name discussed on the mailing list

- Most Preferred:
  - NASR: Network Attestation for Secure foRwarding
  - FELPA: Forwarding Evidence by Local and Path Attestation

- Other Proposals:
  - Network Attestation for Verifiable Forwarding
  - Network Attestation for Dependable Forwarding
  - Attested and Verifiable Forwarding
  - Network Attestation for Verifiable Forwarding
  - Network Attestation for Verifiable Routing
  - NAPA - Network Attestation for Path Accountability
  - Path attestation for Accountable Forwarding - PAF
  - path atteStAtion For accountablE forwarding – SAFE

Next Interim Meeting

- **22 January 2025**
  - UTC 04:00
    - Note: for north America this falls on late Tuesday evening/night (21st January)

Minutes and recording to be posted on github!

Agenda

1. Nancy & Luigi: Meeting opening
   - ○ Any Comment on last meeting minutes?

2. Overview existing Pull Requests on Charter: All
   - ○ https://github.com/ietf-nasr/NASR-Charter

3. New Name for the group: All

If time allows:

1. **NASR Service Model: Meiling Chen**
2. RATS Conceptual Message Wrappers (CMW) in NASR: Henk Birkholz

Agenda

1. Nancy & Luigi: Meeting opening
   ○ Any Comment on last meeting minutes?

2. Overview existing Pull Requests on Charter: All
   ○ https://github.com/ietf-nasr/NASR-Charter

3. New Name for the group: All

If time allows:

1. NASR Service Model: Meiling Chen
2. **RATS Conceptual Message Wrappers (CMW) in NASR: Henk Birkholz**