27 November 2024

NASR Interim Side Meeting

Network Attestation for Secure Routing

This Session is Recorded

Cisco Confidential

Agenda

1. Nancy & Luigi: Meeting opening (5 Minutes)
2. Abstract POT Mechanism – Peter Liu Chunchi
3. NASR & IAB Statement on the Risks of Attestation of Software and Hardware on the Open Internet – Luigi Iannone
4. Document Status & Charter - All

IAB Statement on the Risks of Attestation of Software and Hardware on the Open Internet

- While attestation of client software and hardware is a useful tool for preventing abuse or fraud on the Internet, the **use of such attestation as a barrier to access otherwise open protocols and services would negatively impact the evolution of the Internet as a whole**.
- **For services that have intentionally restricted access, such client attestation (as described in Remote ATtestation procedureS (RATS), RFC 9334) is a valuable security measure**, particularly when used in conjunction with user authentication. However, **this approach is not appropriate for openly accessible services.**
- **Restricting access via attestation of software or hardware would limit the development of new protocols and extensions to existing protocols, lock users into a limited ecosystem of applications, and hamper the ability to audit implementations, conduct measurements, or perform essential security research.**
- **The IAB invites those in the industry and standards community working on client attestation in open services to engage with the relevant IETF working groups (in particular, Privacy Pass and RATS),** and encourages those groups to focus on defining safe deployment models for attestation and abuse prevention that will not put the openness of the Internet at risk.

- **NASR does NOT aim at being used for openly accessible services.**
- **NASR does NOT aim at restricting access to otherwise open services and protocols.**
- **NASR does NOT target wide adoption 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.,**
- **NASR aims at providing auditing tools not access restriction tools.**

- **Where to keep this text? Charter? Wiki? Problem Statement? Other drafts or suggestions?**

Excerpt from: https://datatracker.ietf.org/doc/statement-iab-statement-on-the-risks-of-attestation-of-software-and-hardware-on-the-open-internet/

Document Status – Plans

- Network Attestation for Secure Routing (NASR) Architecture - draft-liu-nasr-architecture-00
  - Peter Chunchi Liu , Meiling Chen , Michael Richardson , Diego Lopez
- NASR Use Case and Requirements - draft-liu-nasr-requirements-02
  - Peter Chunchi Liu , Luigi Iannone , Diego Lopez , Antonio Pastor , Meiling Chen , Li Su
  - Input from Yutaka…
- Terminology and Use cases for Secured Routing Infrastructure draft-richardson-nasr-terminology-01 (Expired)
  - Michael Richardson , Peter Chunchi Liu

Possible New Documents

- NASR Service Model

- Network Attestation for Secure Routing (NASR) Threat Model ?
  - What NASR protect or proves
    - L3-only technology
    - Overlays
  - What NASR does not protect or prove
    - proof of non-transit

- NASR Generic POT ?
  - Design solution that can be encoded in various protocols
    - SRv6
    - MPLS
    - IOAM

Charter

- Now available at:
  - https://github.com/ietf-nasr/NASR-Charter/blob/main/nasr-charter.md

Next Interim Meeting

- 11 December 2024
  - UTC 04:00
  - SAN FRANCISCO 20:00
  - NEW YORK 23:00
  - PARIS 05:00
  - BEIJING 12:00

Minutes and recording to be posted on github!

Minutes from IETF 121

- **General discussion on next steps:**
  - Limited domains seems to be the right approach. Having an Internet-wide deployment, with global trust, is not realistic.
  - Connecting 2 or more limited domains seems feasible as long that there is a mean to ”share” or “transfer” the verification/trust information, via an attestation for instance, so that the verification made in one domain can be continued in another domain. This assumes that domains have specific “agreement” to do so.
  - In the hypothesis that several different requirements exists, this means that different limited domains can use different properties/solutions as long as they agree on the “cross domain attestation”.
  - In case of overlays, it seems meaningful to be able to verify both the overlay and the underlay, as an untrusted underlay makes hardly possible to trust the overlay.
  - We need a crisp definition of the controlled (e.g. SDN) domain boundaries, starting small but keeping in mind the cross-domain extension of the feature set to grow bigger.
  - In order to accommodate the various use cases, the focus should be on generic attributes verification/attestation. The attributes can be a geographic location or a security SLA requirement or anything else. Is not just device trust, rather trust the proof that the device has the requested attributes.
  - We should give negative examples. Like the fact we can catch situation where routing would forward packets through boundaries that are not acceptable the specific use case (slide 6 untrusted black router). It is not that there is an error in routing. Traffic with no specific requirements can follow that path.
- **High priority action points:**
  - Refine the scope and problem statement
  - Terminology: even during the side meeting terminology was somehow not completely aligned among the participants
  - Start thinking about a charter proving that the problem is relevant for the IETF and that can be solved.