Network Attestation for Secure Routing Recaps and Updates

IETF 121

Dublin, Nov 4, 2024

Chunchi (Peter) Liu

liuchunchi@huawei.com

Updates

- Fixing the diagrams
- Adding of new concept:
  - Forwarding Baseline: A deterministic reference value that can be used in the path validation process.

- Generic method to describe POT mechanisms
  - POT mechanism is hard to converge
    - People has different designs
    - Different administrative domains want to use different methods
  - But still we want them to work together
  - Develop generic message types, roles and protocols that help them work together

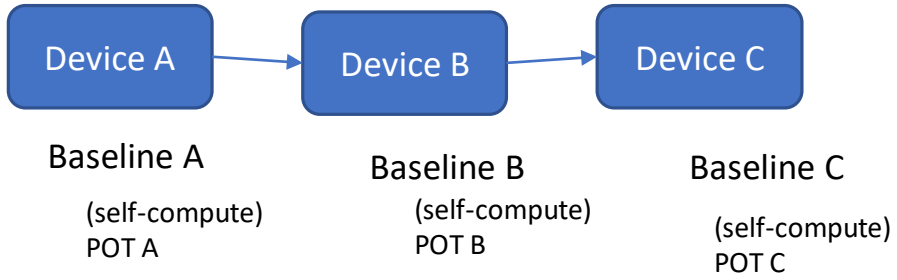
POT Mechanism

- Verification Points
  - Intermediate nodes (of a path), destination node (of a path), controller
    - Normal routers, domain egress gateway
- POT-updating Points
  - Intermediate nodes (of a path)

- POT Baseline -- reference value to verify an actual POT.
  - Controller-issue or self-dial-test-compute
- POT – actual proof-of-transit carried in the packet or sent out-of-band, computed by POT-updating Points

? Where to encapsulate the POT: IOAM/AH/OOB

? Need a new draft to describe generic POT



Recapping and lesson learned

- Domain – within limited domain, connecting 2 limited domains
  - Roman: limited domain, yes; cross domains/internet, emm
- Problem:
  - Verifying and auditing/proving forwarding compliance against a given baseline
- Assumptions:
  - Devices are attestation ready -- devices can be descried as claim sets or AR4SI
  - Devices operate in a SDN-controlled, SRv6 ready network (backbone, metro)
- Use Cases:
  - Traffic not go out of country (or a certain domain)
  - Traffic transmit on top of devices only with certain attributes (security SLA assurance)
    - Deb and crowd: focus on critical use cases

```
     +---------------+
     |               |
     | Relying Party |
     |               |
     +-+---------^---+
Path   |         |
Request|         | Report
       |         |
     +-v---------+--+                          +-----------+
     |              |      Path Attestation    |           |
     | Orchestrator |       Result (PAR)       | Verifier  |
     |              <--------------------------+           |
     +-+------------+                          +------^----+
       |                                              |
       | Path                                         |  Path
       | Evidence                                     |  Evidence
       | (PE)                                         |  (PE)
     +-v------------+      +-------------+     +------+----+
     |              |      |             |     |           |
     |   Attester   +------>  Attester...+-----> Attester  |
     |              |      |             |     |           |
     +--------------+      +-------------+     +-----------+
                  Update with         Update with
                   AR/RE/PoT           AR/RE/PoT
```

```
+-----------------------------------+
|                                   |
| Client X                          |
|            Path    +-----------+  |
| +----------+Evidence| Relying   |  |
| | Attester |<-------+ Party     |  |
| +--+-------+        +---^--+----+  |
+----+--------------------+--+-------+          +-------------+
     | Update       Answer|  | Path             |             |
     | Path         Report|  | Request          |             |
     | Evidence           |  |                  |  Vendors    |
+----+--------------------+--+-----------+      |             |
|    |                    |  |           |      |             |
|    |                    |  | Operator 1|      |             |
|    |                    |  |           |      |             |
| +--v--------+  RE   +---+--v--------+  |  RE  |+-----------+|
| |           +------->               +--+------>| Verifier  ||
| | Attester  |       | Orchestrator  |  |      || Vendor A  ||
| | Vendor A  <-------+               <--+------++           ||
| +--+--------+  AR   +------+--------+  |  AR  |+-----------+|
+----+-----------------------+-----------+      |             |
     | Update                | Intra            |             |
     | Path                  | ISP              |             |
     | Evidence              | API              |             |
+----+-----------------------+-----------+      |             |
|    |                       |           |      |             |
|    |                       | Operator 2|      |             |
|    |                       |           |      |             |
| +--v--------+  RE   +------v--------+  |  RE  |+-----------+|
| |           +------->               +--+------>| Verifier  ||
| | Attester  |       | Orchestrator  |  |      || Vendor B  ||
| | Vendor B  <-------+               <--+------++           ||
| +--+--------+  AR   +---^-----------+  |  AR  |+-----------+|
+----+--------------------+--------------+      |             |
     | Update             |   Path              |             |
     | Path               |   Attestation       |  ...        |
     | Evidence           |   Result (PAR)      |             |
+----+--------------------+----------+          |             |
|    |        Path        |          |          +-------------+
| +--v-------+Evidence+---+-------+  |
| | Attester +--------> Relying   |  |
| +----------+        | Party     |  |
|                     +-----------+  |
|  Client Y                          |
+-----------------------------------+
```

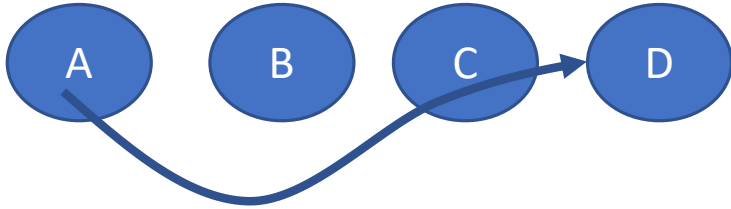
Paths in trusted domains

- If we operate in limited/trusted domains, do we still need to distinguish paths?
- Yes:

Without RATS	
Security Assumption of Devices	Limitations
Not trusted/no trustworthiness Internet	Correctly propagated routing information does NOT guarantee correct forwarding
Completely trusted Limited Domains	Is your device *really* unconditionally trustworthy? • Security by obscurity is bad

With RATS
Security Assumption of Devices
• Device has different trustworthiness properties • Finer-granularity of discretion is now possible Limited Domains
Important flow Limited Domains

SAVNET vs NASR



- Verify the origin VS Verify the first-half path
  - SAVNET: Each device maintain a table |origin|ingress interface|
  - NASR: Each device maintain a verifiable baseline, using which can verify all hops before
  - Value-add: fix re-route attack

- Verify the route origin VS Verify the attributes of the first-half path
  - SAVNET: No considerations of device attributes verification
  - NASR: Verify intermediate device attributes/properties on the fly
  - Value-add: Verify path (trust) attributes/properties

- Interdomain SAVNET VS Interdomain NASR

Other issues

- Verifier interop
  - If the verification point is at the intermediary nodes, how and why should the node j believe the verification result of node i?

- Generic POT draft
- Cross operator API – what to send?
  - POT baseline, “path id”, aggregated ARs, keys…
- Service Model?
- Side Meeting reports to SEC ADs before BOFREQ