On Path Validation and a Possible Solution

draft-liu-on-network-path-validation-00

HotRFC Lightening Talk @ IETF 117, July 2023
Chunchi Liu (Huawei)
Why do we care about path validation?

Routing Security Attacks
- Routing Hijack
- Route Injection
- Route Leak
- Denial of Service

Foster

Secure route propagation and authentication in the control plane
- BGPSec
- RPKI
- ...
  - Is it enough?

Mitigate

Cannot guarantee the planned path is actually used

Enforcing and verifying the correct transit of traffic in the data plane
- Path Validation
- draft-ietf-sfc-proof-of-transit
- ...

Provide transit proof to complement

What is Path Validation?
- Path validation is a mechanism that "ensures" data packets strictly traverse the chosen network path.

The desired path

The actual path
In Internet routing, the *actual* path the traffic took may *not* be the path we *planned*

- Alice is having a **confidential** business video meeting or VOIP call.
- She doesn’t want any data of this connection be detoured and monitored.

![Diagram showing network routing and security measures](image)
A Graphical Overview of the VC-based Path Validation Solution

**Security**

- **Position-binding property**: Transit proof $P_i$ successfully passes verification \iff it was created by the right node $n_i$ at the right position $i$ as previously committed

**Advantages**

- **Efficient**: Proof creation and verification takes $O(1)$ time
- **Succinct**: Transit proof and commitment is $O(1)$ size
- **Batch-proof** friendly (same efficiency)

**Stage 1: Compute Reference Value**

Network Controller

- Controller selects a path
- Computes a commitment

**Output 1**

Commitment

$C$

$R_1 R_2 R_3 R_4$

**Stage 2: Generate Transit Proof**

Router $R_i$

- Forwards data
- Computes his transit proof $P_i$

**Output 2**

Transit Proof

$P_i$

$R_1 R_2 R_3 R_4$

**Stage 3: Verification**

Verify($C, P_i$) = $1$

- Observer verifies $P_i$ against $C$ to check if it was the correct router in correct position.
Anti-detour security-sensitive communication

- Alice is having a **confidential** business video meeting or VOIP call.
- She doesn’t want any data of this connection be detoured and monitored.

- **Position-binding:** Malicious node at incorrect position cannot compute a correct transit proof, halting the connection and alarming the owner.
Looking for interested collaborators to:

1. Work on the draft
2. Joint research for a lot of extending work
3. Conduct joint PoC implementation and deployment test

On **OPSEC**

Thursday 7.28
15:30 - 16:30

draft-liu-on-network-path-validation

Chunchi Liu, liuchunchi@huawei.com
liuchunchi.com

Please don’t hesitate to catch me in the venue :)