Path Validation Gap Analysis

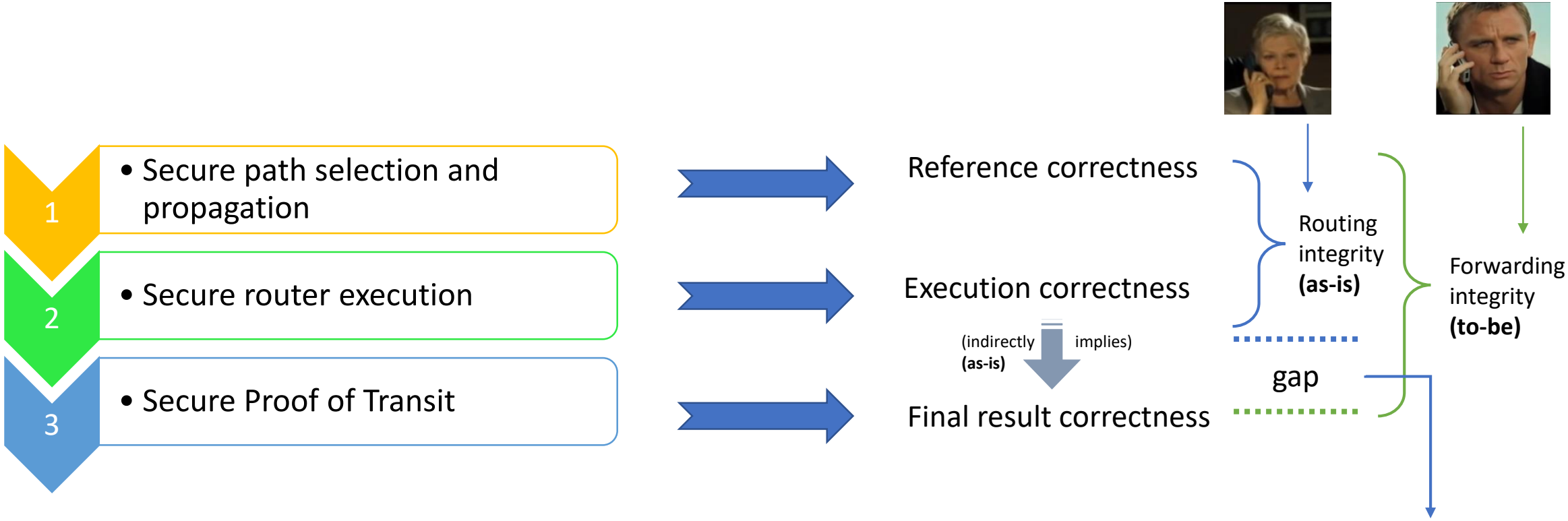
Huawei

IETF 118

Gaps

- **Routing Integrity vs Forwarding Integrity**
- Path Validation vs Proof of Transit
- BGP scenario vs more scenarios

Gap 1: Routing Integrity vs Forwarding Integrity



Three-step recipe to secure routing

To **directly** fill this gap, we need **proof-of-transit** mechanisms.

Existing efforts to connect the gap

1. Telemetry: IOAM/IFIT/Path tracing

2. Proof of transit

3. Path reconstruction
   - Reconstruct forwarding path by collecting router forwarding configuration data

The common blocker is a general Proof of Transit solution!
Or does different scenarios require different solutions?

The Good	The Bad
• Allow **underlay** network data telemetry	• **Not applicable to virtual paths** composed of network functions • **Need secure POT** as building block
• **Works for both** for **virtual paths** like SFC and **underlay path**.	• Could pose computational and packet **overhead.** • Inability to perceive **stealth nodes**.
• No data plane modification	• **Indirect way** of verifying forwarding outcome, **inferior than secure POT.** • Need admin access to all routers • No drafts, just research papers

Gaps

- Routing Integrity vs Forwarding Integrity
- **Path Validation vs Proof of Transit**
- BGP scenario vs more scenarios

Gap 2: Path Validation vs Proof of Transit

- Path Validation:
  - **Old** Interpretation:
    - Validating the planned path is a trusted, authorized path.
    - **Control plane** path validation, **before** forwarding.
      - Mostly used in BGP context, validate AS-path.
  - **New** Interpretation:
    - Validating what paths a packet has actually traversed.
    - **Data plane** path validation, **after** forwarding.
      - Mostly used in research papers.

Disambiguates into → Proof of Transit

Conclusion:

- Path validation **scope** = **old** + **new** = Routing Integrity + Proof of Transit = Forwarding Integrity
  - Path validation should include proof of transit.
- Proof of Transit **goal** is to achieve verifiable assurance of hop-by-hop forwarding integrity!

Gaps

- Routing Integrity vs Forwarding Integrity
- Path Validation vs Proof of Transit
- **BGP scenario vs more scenarios**

Gap 3: BGP scenario vs more scenarios

- Path Validation:
  - **Old** Interpretation:
    - Validating the planned path is a trusted, authorized path.
    - **Control plane** path validation, **before** forwarding.
      - Mostly used in BGP context, validate AS-level path.
  - **New** Interpretation:
    - Validating what paths a packet has actually traversed.
    - **Data plane** path validation, **after** forwarding.
      - Mostly used in research papers.

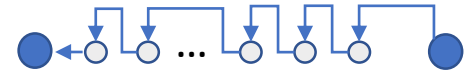
RPKI

BGPSEC

What does it do?

Validates: Is **origin AS** authorized to announce ownership to an IP prefix in BGP update?

Validates: Is **every AS on the AS path** of a BGP route announcement has explicitly authorized this **route advertisement**?



Gap 3: BGP scenario vs more scenarios

- Path Validation:
  - **Old** Interpretation:
    - Validating the planned path is a trusted, authorized path.
    - **Control plane** path validation, **before** forwarding.
      - Mostly used in BGP context, validate AS-level path.
  - **New** Interpretation:
    - Validating what paths a packet has actually traversed.
    - **Data plane** path validation, **after** forwarding.
      - Mostly used in research papers.

RPKI

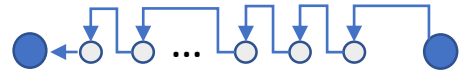
What does it do?

Validates: Is **origin AS** authorized to announce ownership to an IP prefix in BGP update?

Origin AS Validating AS

BGPSEC

Validates: Is **every AS on the AS path** of a BGP route announcement has explicitly authorized this route advertisement?



Origin AS Validating AS

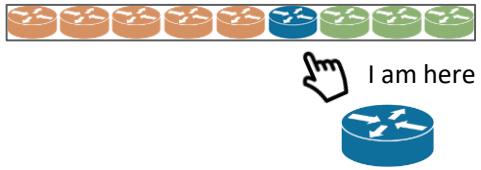
gap

BGP also does not have POT solution.

Gap 3: BGP scenario vs more scenarios

- Why path validation should not be limited to AS level and BGP?

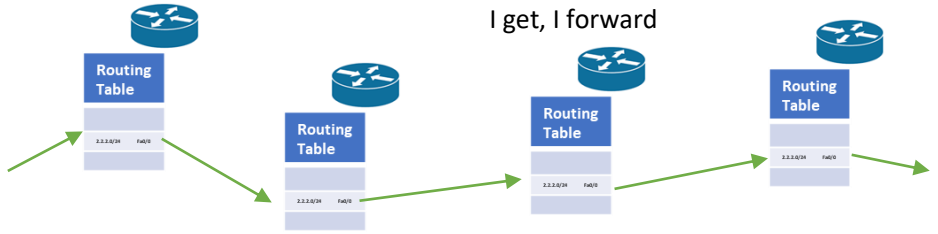
Explicit Routing: Protect the forwarding integrity on the **explicit path.**



Benefits:

- Service Function Chaining
- Segment Routing
- Path Aware Networking (SCION)

Conventional Routing: Protect the forwarding integrity on the **implicit path** implied by the routing table.



Benefits:

- Policy-based Routing (BGP Flowspec)
  - Routing policy compliance check
- Multipath (BGP link bandwidth, ECMP/TE)
  - Locate exact path the traffic actually took among all valid paths. Quick switch when one path went bad.
- IOAM/IFIT

Gap 3: Some **Immediate** Technical Benefits

Benefitting Techniques	Value-add of path validation	Related Drafts
• Service Function Chaining/WIMSE	• **Proof of Virtual Function Processing** • Proof of API/Microservices/Container Processing	draft-ietf-sfc-proof-of-transit
• Segment Routing/MPLS	**More accurate path tracing/logging/marking** • Transitive transit proof	RFC 9343, draft-filsfils-spring-path-tracing draft-filsfils-spring-path-tracing-srmpls
• IOAM/IFIT	**More accurate telemetry** • In-situ or individual packet	RFC 9197, RFC9378, RFC9452 draft-song-opsawg-ifit-framework
• Ingress Filtering	• **Augment uRPF check** by executing an actual path backward traversal, not just a FIB lookup, reduce false negative rate. • Or filter packets by checking the transit proof it carries.	RFC3704, RFC8704, RFC5635 draft-xu-ipsecme-risav
• Policy-based Routing	**Compliance check**: is policy correctly enforced at every router?	RFC1104, RFC9067
• Multipath (ECMP/TE)	Know which path it actually took among all valid paths, when one path went bad, **quickly locate the problematic path** and switch to other paths.	RFC6754
• ALTO	**Add a trust metric** using the result of path validation to ALTO path selection (Trust-enhanced networking).	RFC7286
• RATS	Use path validation result to **verify and attest a path**, instead of attesting just one device.	RFC9334

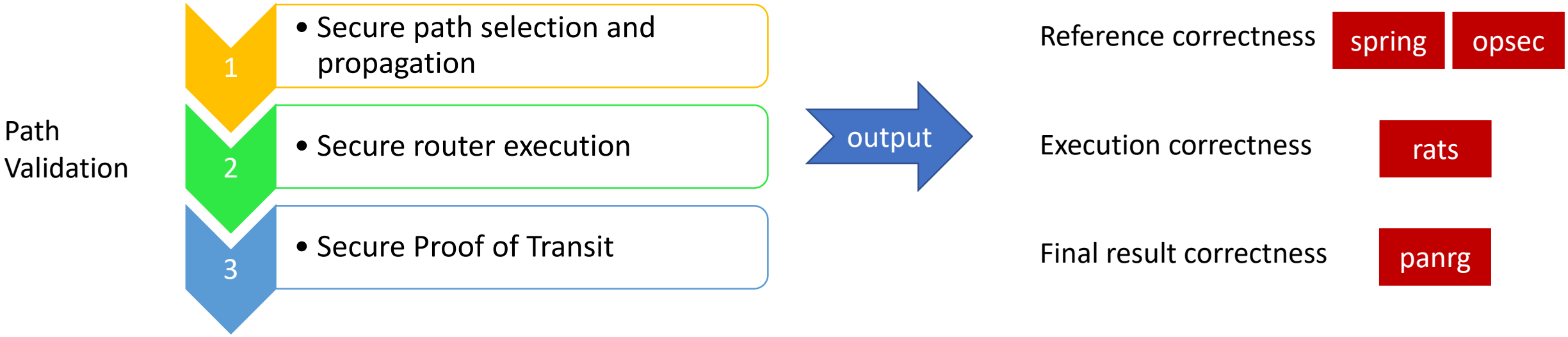
Do we need design team to these blockers?

- Intra-domain POT, Inter-domain POT, POT utilizing RPKI, … many different scenarios!
- Definition of trust metrics of a path.

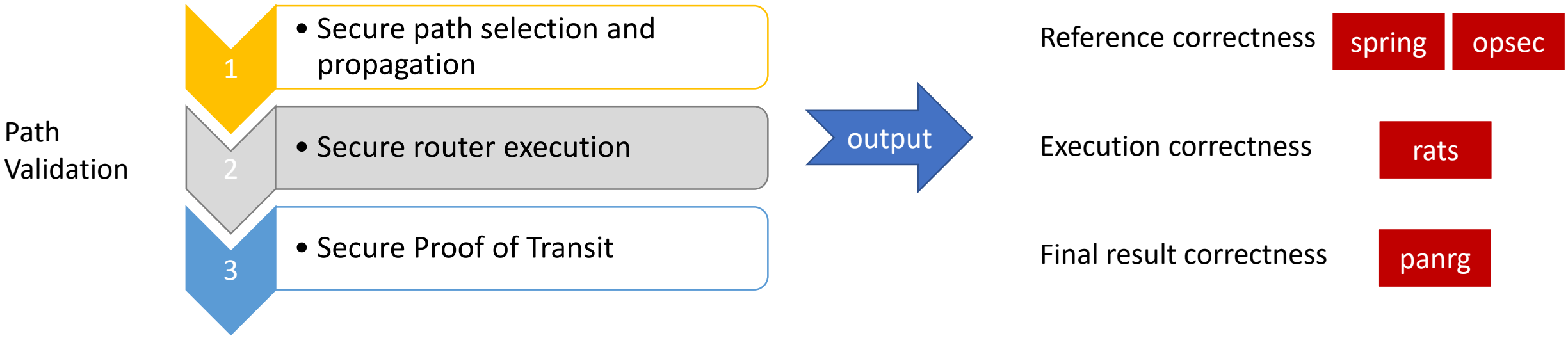
Conclusion: Gaps

- Routing Integrity vs Forwarding Integrity
  - **Main reason:** Control-plane security techniques can only achieve routing security and *imply* forwarding integrity.
  - **How to fix:** Design proof of transit solutions to directly verify the forwarding result.
- Path Validation vs Proof of Transit
  - **Main reason:** Long history of term misuse and confusion.
  - **How to fix:** Clarifies scope of path validation. Now path validation includes POT.
- BGP scenario only vs more scenarios
  - **Main reason:** Lack of attention and use case discussion.
  - **How to fix:** Agree on valid use cases that can greatly benefit from path validation.

Potential Overlaps with Existing WGs



Potential Overlaps with Existing WGs



What are the out-of-scopes?

- **Illegal data copy:** Data obtained by a router is illegally copied by its owner and sent elsewhere.
  - Data is intangible in nature. This is a data watermark problem.

- **Stealth nodes:** inferior nodes not perceivable in the current layer
  - Layered design of Internet purposely make inferior nodes not perceivable. It does not make sense and violates layered design principle trying to perceive stealth nodes. To the very least, it is a different problem.
  - Stealth nodes in most of the times are not significant security threats. They are just either old or computationally weak.
  - One step ahead is better than no progress.

Gap analysis ends here

Any questions before open discussion?

Discussion:

The floor is open for discussion.

Questions
Question 1: Do you agree there is a gap between routing integrity and forwarding integrity, and the gap exists due to the lack of a secure proof-of-transit solution? • Do we need different answers for different scenarios ?
Question 2: Should path validation's scope include the following: 1. Validating the planned path is a trusted, authorized path (control plane, before forwarding) 2. Validating what paths a packet has actually traversed (data plane, after forwarding) Or do you think path planning and attestation according to the device/function trustworthiness should also be part of the scope?
Question 3: Is this an IETF problem? Does it belong to SEC area, OPS area or RTG area? Which WG or WGs should abovementioned works be done in?
Question 4: Do you agree our next steps should include: 1. Collaborate and improve the problem statement draft 2. Design secure proof-of-transit solutions 3. Standardize mechanisms that can evaluate and select a path by its trustworthiness Missing anything?