APNIC 62 · MUMBAI

The Good Neighbor Problem

BGP Security Beyond Your Own Prefix

Dr. Ritesh Mukherjee

RPKI/ROV · ASPA · BMP

16 June 2026 — 07:17 UTC

AS18101

A black hole meant for a domestic block starts announcing someone else's prefix — origin: AS62041, Telegram.

Within minutes, it's on RIPE RIS in Amsterdam.

The Cascade

India orders a temporary Telegram block (NEET-UG exam-leak probe)

▼

AS18101 (Rcom) originates 91.108.4.0/22 — Telegram's own prefix — to blackhole it domestically

▼

Announcement isn't scoped to India — propagates onto global eBGP

▼

Visible on RIPE RIS RRC01 within minutes — real hijack, not a rumor

▼

Telegram fights back with more-specifics — AS18101 hijacks those too, hours later

The Impact

UAE	Middle East users lose reachability to Telegram entirely
EU	European vantage points observe the hijacked route too
2x	Round two — Telegram's counter-announcement gets hijacked
150M	Indian users already affected by the underlying domestic block

TECHNICAL BREAKDOWN

What was missing

No scope on the black hole

A domestic RTBH-style announcement went out via eBGP without community tagging or filtering to keep it within India.

Origin ≠ prefix owner

AS18101 originated a prefix that RIPE-delegated AS62041 (Telegram) had never authorized it to announce — a textbook origin hijack.

Round Two, same mistake

When Telegram fought back with more-specifics, AS18101 hijacked those too — no lesson learned between round one and round two.

This is, mechanically, a plain origin hijack — the kind ROV was built to stop. The question is not whether ROV can catch it. It's whether the AS in the path chose to check.

ROV Would Have Worked — If Enforced

Telegram's prefixes carry ROAs. Any network that validates origin against RPKI will drop AS18101's announcement outright.

WOULD HAVE CAUGHT IT

ROV, if enforced on the path. Origin AS18101 doesn't match the ROA for 91.108.4.0/22 — an unambiguous Invalid.

Prefix filtering at IX/peering points that rejects announcements for prefixes a peer has no business originating.

WHY IT DIDN'T

Only ~27% of ASes globally enforce ROV. The other 73% pass through whatever the origin claims.

India's own ROV enforcement sits near zero (more on this shortly) — the leak had a clear path out before it reached anyone who validated it.

SINGAPORE / PHILIPPINES · FEBRUARY–APRIL 2025

The Hijack Nobody Saw — Including the Victim

A sub-prefix of SingNet's own address space gets hijacked. The victim's own routing table never shows it. Traffic still gets diverted.

AS3758

SingNet — legitimate origin of 203.127.0.0/16

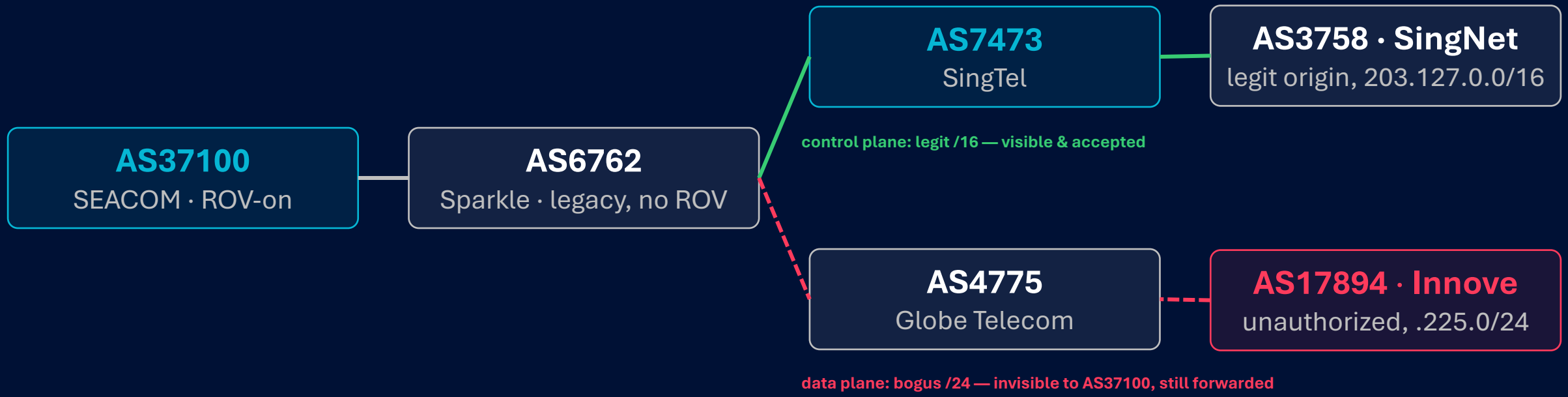
AS17894

Innove Comm. — announces 203.127.225.0/24, unauthorized

AS37100

SEACOM — ROV-enabled vantage point, 100% filtering rate

Same Internet, Two Different Views



AS37100 drops the bogus /24 (good ROV) — but AS6762 doesn't, and forwards anyway

traceroute to 203.127.225.1 still lands in AS1789

Partial ROV Deployment Creates a Blind Spot

THE MECHANISM

AS37100 validates and correctly drops the invalid /24. Its own routing table looks clean — **no reason to suspect anything is wrong**. But traffic still transits AS6762, a non-validating AS in the same path, which accepts the bogus route and forwards it to AS17894. Control-plane visibility and data-plane reality diverge — silently.

THIS ISN'T RARE

A large-scale study of exactly this pattern found **318 high-confidence stealthy hijacking incidents** across **2,178 unique routes** on today's Internet. Reported to Globe Telecom on 10 Feb 2025; still observed on 24 April 2025 — **over two months with nobody the wiser**.

The more networks that partially deploy ROV, the more of these inconsistent views appear — partial adoption doesn't fail safely, it fails invisibly.

16 April 2021 — 13:40 UTC — Mumbai

824 → 37,739

That's how many prefixes AS55410 (Vodafone Idea) normally originates — and how many it suddenly originated instead.

Almost none of them belonged to Vodafone Idea.

The Cascade

A misconfiguration — likely a route optimizer or traffic-engineering test — causes AS55410 to originate prefixes it doesn't own

▼

Upstream Bharti Airtel (AS9498) has no prefix limit and no AS-path filter on the session — passes everything through

▼

Announcements reach RIPE RIS and RouteViews within minutes — a genuinely global anomaly

▼

234 RIS peers and 162 RouteViews peers observe the hijack — and Vodafone Idea's own network is inundated by the return traffic

The Impact

37,739	prefixes hijacked — up from a baseline of 824
164	countries affected
4,012	ASNs affected
13x	spike in inbound traffic to Vodafone Idea itself

WHAT WAS MISSING

Three Layers, All Absent

No RPKI ROV in the path

Nearly every one of the 37,739 prefixes had a real owner elsewhere, with a valid ROA in many cases. Origin validation at any hop would have flagged them as invalid.

No prefix limit at Airtel

Vodafone Idea had never originated more than ~824 routes. A prefix-limit circuit breaker on the Airtel session would have shut this down in seconds.

No AS-path / IRR filtering

Other upstream peers didn't propagate the bad announcements — Airtel's session was the one weak link that let it go global.

Unlike a stealthy hijack, this one was loud, global, and visible on every collector within minutes — and still ran for roughly ninety minutes before it was cleaned up.

This One Is Squarely in RAVEN's Lane

Same enforcement gap as Telegram/Rcom — just bigger, older, and carried by a Tier-1 regional upstream instead of a domestic black hole.

WOULD HAVE CAUGHT IT

ROV at any hop — Airtel, a downstream peer, anyone — drops origin-invalid announcements the moment they don't match a ROA.

Prefix-limit hygiene at Airtel would have capped the blast radius, even without RPKI in the picture.

WHY IT DIDN'T

2021, and still true in 2026 — India's ROV enforcement sits near zero (0.99%, coming up shortly). The gap that let this through hasn't meaningfully closed in five years.

No circuit breaker on the one upstream session that mattered.

NOT THREE INCIDENTS. A PATTERN.

Eighteen Years, One Region, Same Story

2008 **Pakistan Telecom (AS17557)** hijacks YouTube to enforce a domestic block — leaks globally; YouTube goes dark worldwide for ~2 hours.

2010 **China Telecom (AS23724)** misannounces ~50,000 prefixes; widely reported as 15% of global traffic rerouted through China for 18 minutes (later analysis disputes the true traffic share, but the routing anomaly itself is undisputed).

2015 **Bharti Airtel (AS9498, India)** route leak — 2,000+ AS networks affected for up to 9 hours across India, China, the US, Japan, and Saudi Arabia.

2021 **Vodafone Idea (AS55410, India)** originates 37,739 foreign prefixes across 164 countries, affecting 4,012 ASNs, all carried globally by Bharti Airtel with no filtering. Covered in detail shortly.

2025 **Innove Comm. (AS17894, Philippines)** stealth-hijacked SingNet's sub-prefix — invisible on the victim's own control plane for over two months.

2026 **Rcom (AS18101, India)** hijacks Telegram's own prefixes, trying to enforce a domestic block — leaks to the UAE and Europe.

Three Failure Modes, One Region

INCIDENT	FAILURE CATEGORY	WHAT WOULD HAVE STOPPED IT
Telegram / Rcom, 2026 · Vodafone Idea, 2021	ROV enforcement gap	Origin validation, if enforced anywhere in the path — plus prefix-limit hygiene at the upstream
SingNet / Innove, 2025	Detection gap under partial ROV	Data-plane / BMP-correlated monitoring — control plane alone missed it for 2+ months
Bharti Airtel, 2015	Route leak, no path validation	ASPA — customer-to-provider relationship was never declared
Pakistan Telecom, 2008 · China Telecom, 2010	Unscoped origin hijack, global leak	ROV + peer-level prefix filtering

This region isn't an unlucky bystander.

It's structurally exposed — as both source and victim.

Every incident on the last two slides has an APNIC-region AS at the origin or as the victim. Let's look at why.

GLOBAL RPKI DEPLOYMENT · MID-2026

Signed ≠ Validated

67.2%

of routed prefixes carry a ROA globally (Hurricane Electric, 26 Jul 2026) — IPv6 at 73.5%, IPv4 at 65.6%.

26.9%

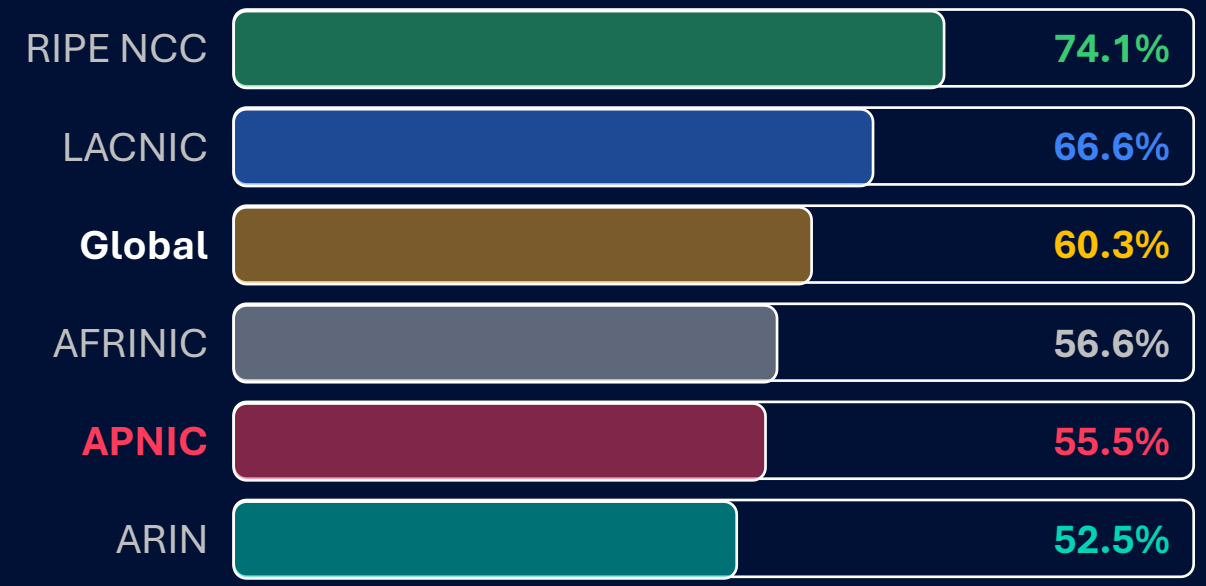
of ASes globally actually enforce ROV — publication has outpaced enforcement almost everywhere.

6000+

RPKI-invalid prefixes still observed per day, even with majority ROA coverage (CableLabs / Qrator).

Origin authorization is mainstream. Path authorization — ASPA — has barely started. And enforcement of what's already signed remains the weak link everywhere.

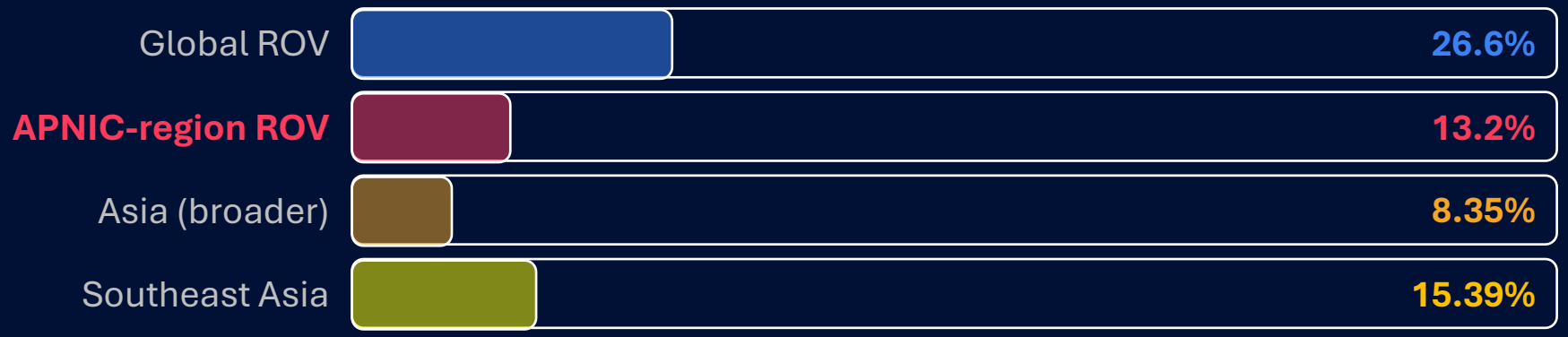
ROA Coverage by RIR (IPv4 Valid %) — Feb → mid-2026



On IPv6, the gap is worse: APNIC sits at 45.2% valid, compared with 81.5% for RIPE NCC and a 60.9% global average.

Source: APNIC Labs / NIST RPKI Monitor, presented at APRICOT 2026.

The Enforcement Gap Is Worse Than the Signing Gap



PNIC-region ROV enforcement is roughly half the global rate. In parts of the region, it's roughly a third of the global rate. This is exactly the gap the Telegram/Rcom and Pakistan Telecom incidents walked through.

Not Uniform — Some Economies Are Pulling Ahead

✓ Doing well

- **Indonesia** — ROA coverage 66.0% → 90.6% in 3 months; ROV ~21.7%
- **Vietnam, Philippines, Malaysia** — driving SE Asia ROA coverage to ~90.7%
- **Myanmar** — subregional ROV leader at 62.6%
- **India (ROA only)** — 88.0% IPv4 / 97.9% IPv6 ROA coverage

✗ Falling behind

- **India (ROV)** — just 0.99% of networks filter invalid routes, vs 3.14% in South Asia and 26.9% globally
- **Asia overall** — 8.35% ROV vs 21.6% global average
- **Pacific Islands** — 49 of 116 routable ASNs show some exposure, most relying entirely on upstream filtering
- **ASPA** — effectively 0% enforcement anywhere in the region

India Signs. India (Mostly) Doesn't Validate.

88.0% IPv4 ROA coverage

vs

0.99% ROV enforcement

This is precisely the gap that let AS18101's hijack of Telegram's own, properly-signed prefixes leak past everyone who should have caught it. The ROA existed. Almost nobody checked it.

THE ROUTING SECURITY STACK

Three Layers of Defense

3 — BMP — Telemetry & Anomaly Detection
Does your control plane actually match the data plane?

2 — ASPA — Path Validation
Does the AS_PATH reflect legitimate provider relationships?

1 — ROV — Route Origin Validation
Is the origin AS authorized to announce this prefix?

Plus operational hygiene underneath all three — max-prefix limits and overload protection.
No single layer is sufficient on its own.

LAYER 1

ROV: Necessary, Enforcement - Dependent

CATCHES

Plain-origin hijacks — Pakistan Telecom 2008, Telegram/Rcom 2026. Covers most accidental and opportunistic hijacks.

OPERATIONAL NOTE

Drop invalids, don't downpref — downpref keeps the invalid reachable via a longer path. Run 2+ validators for redundancy.

MISSES

Route leaks, forged-origin path manipulation, and anything where the intermediate AS doesn't enforce — the SingNet/Innove blind spot.

REGIONAL REALITY

PNIC-region enforcement (13.2%) is half the global rate. This layer is signed but largely unused across the region.

LAYER 2

ASPA: Closes the Path-Validation Gap

CATCHES

Route leaks through transit — Bharti Airtel 2015, Vodafone Idea 2021. A customer-to-provider relationship that was never declared shows up as ASPA-invalid.

STATUS TODAY

Object creation is live in APNIC, RIPE NCC and ARIN. Standards track: draft-ietf-sidrops-aspa-verification. Enforcement in the wild is effectively 0% globally — and 0% in APNIC's region specifically.

MISSES

Origin hijacks (that's ROV's job) and anything inside a single AS's own control plane — pure operational-hygiene failures.

WHY IT MATTERS HERE

Two of the region's largest leaks (2015, 2021) were exactly the shape ASPA is designed to catch — a wrong upstream relationship, not a wrong origin.

LAYER 3

BMP: The Layer That Would Have Found the Invisible Hijack

CATCHES

Exactly the SingNet/Innove pattern — a mismatch between what your control plane believes and what your data plane actually forwards.

WHY IT MATTERS

The SingNet hijack ran undetected for 2+ months via control-plane monitoring alone. Streaming Adj-RIB-In and correlating against expected origins turns "months" into "seconds."

MISSES

Nothing on its own — it's a detection layer, not a prevention layer. Value depends on someone watching the correlated output.

STANDARD

RFC 7854, an RFC since 2016. Mature, widely implemented, and still rarely deployed for security correlation rather than raw stats.

What Each Layer Actually Catches

THREAT	ROV	ASPA	BMP
Plain origin hijack (Pakistan Telecom, Telegram/Rcom)	✓	✗	◐
Mass origin hijack, unfiltered by upstream (Vodafone Idea)	✓	✗	◐
Route leak through transit (Bharti Airtel)	✗	✓	✓
Stealthy hijack under partial ROV (SingNet/Innove)	◐	✗	✓
AS_PATH forgery behind a legitimate origin	✗	✓	✓

◐ = partial or detection-only, not prevention. Operational hygiene — max-prefix limits, overload protection — sits underneath all three layers and is covered in the checklist ahead.

OPEN SOURCE · NOKIA/BGP-ROUTING-SECURITY-MONITOR

RAVEN

Routing Analysis, Validation, and Event Network — a single binary that correlates BMP, RPKI ROV, and ASPA path validation into one operator-facing security posture.

BMP

Embedded receiver — zero external dependencies for your first annotated route.

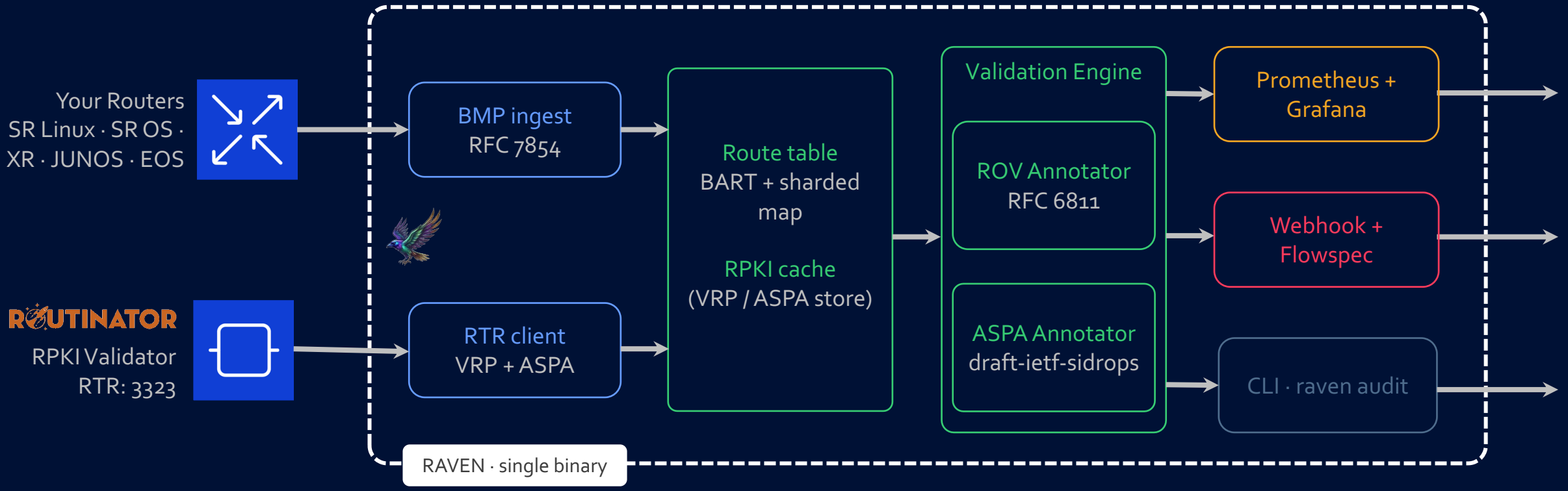
ROV + ASPA

Every route gets one combined posture, not two checks you reconcile by hand.

IMMEDIATE

go install and point it at your router — real-time queries from day one.

BMP In. RPKI Checked. One Posture Out.



No mandatory external dependencies.One binary, one config file.

ILLUSTRATIVE OUTPUT · NOT A LIVE DEMO

What This Would Have Looked Like

Telegram / Rcom pattern — raven watch

```
$ raven watch --posture origin-invalid
[07:19:02] 91.108.4.0/22 via 10.0.0.1 origin:AS18101
  ROV:Invalid — expected AS62041 per ROA
  posture:origin-invalid → dropped if reject-invalid is enforced
```

SingNet / Innove pattern — raven audit

```
$ raven audit --prefix 203.127.0.0/16
control-plane: 203.127.225.0/24 — not present (ROV dropped it)
BMP data-plane hint: next-hop churn on covering /16
  flag: origin/path mismatch vs peer AS37100's own view
```

HARDENING CHECKLIST

This Quarter — Quick Wins

Set max-prefix limits on every eBGP peering session.
The missing circuit breaker in the Vodafone Idea/Airtel hijack. Prevents a flood — accidental or malicious — from ever reaching your core.

Create ROAs for every prefix you originate.
Match exactly what you announce. Be careful with maxLength.

Enable ROV on all eBGP sessions — drop invalids, don't downpref.
This alone would have stopped the Telegram/Rcom and Pakistan Telecom hijacks.

Cross-check your control-plane view against a second vantage point.
Looking-glass or traceroute spot-checks catch what your own table can't show you.

HARDENING CHECKLIST

This Year — Build the Stack

5 **Sign your ASPA object in APNIC / RIPE NCC / ARIN.**
List every transit provider. Keep it in sync with upstream changes.

6 **Deploy BMP to stream Adj-RIB-In to a collector.**
RAVEN, pmacct, OpenBMP, or commercial. Start with one border router.

7 **Correlate BMP with RPKI state — alert on origin/path mismatches.**
This is exactly what would have surfaced the SingNet/Innove hijack in seconds, not months.

8 **Join MANRS and share your baseline with the community.**
Routing security is collective — your defenses help your peers, theirs help you.

Resources & Tools

Check your status

isbgpsafeyet.com

stats.labs.apnic.net/rpki

rpki-monitor.antd.nist.gov

bgp.tools

Deploy RPKI & ASPA

MyAPNIC → RPKI

RIPE NCC RPKI Dashboard

ARIN Online → RPKI

nro.net/rpki-best-practices

RAVEN & BMP

github.com/nokia/bgp-routing-security-monitor

ritmukhe.github.io/raven-docs

RFC 7854 (BMP)

Key Takeaways

This is a pattern, not a string of bad luck.
Six major incidents, eighteen years, one region — as both source and victim.

The region signs more than it validates.
India: 88% ROA, 0.99% ROV. APNIC-region ROV is half the global rate. That gap is where every hijack in this talk got through.

Build the full stack: hygiene, ROV, ASPA, BMP.
Each layer covers what the others miss — and the "stealthy hijack" pattern shows partial deployment can be worse than none.

Routing security is collective and regional.
Your defenses protect your neighbors. Their gaps — in the same region — expose you.

Signed, Filtered — and Still Vulnerable

unless you build the full stack.

Dr. Ritesh Mukherjee

APNIC 62 · MUMBAI · SEPTEMBER 2026