~~The Peering Black Hole~~

RPKI Wahala

How RPKI Hijacks Your Traffic

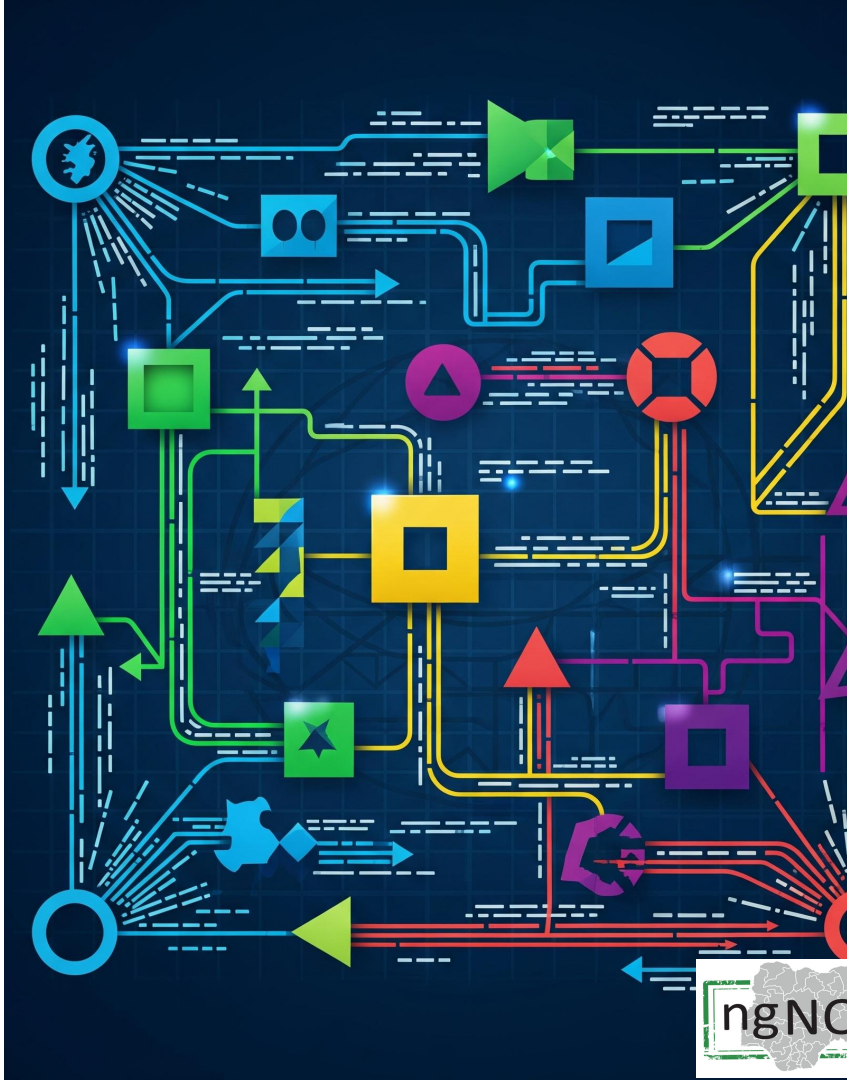
Your network has a high-capacity, direct peering link, but crucial traffic destined for it seems to vanish, only to reappear on congested, high-cost transit paths. Perfectly good infrastructure is silently bypassed. What's hijacking your traffic?

This presentation touches on a likely culprit:
RPKI (Resource Public Key Infrastructure).

While designed to secure BGP, **simple misconfigurations** in your Route Origin Authorizations (ROAs) can cause your legitimate route announcements to be marked as "Invalid."

These days, peering partners like <<*insert favourite large content provider*>> will drop these routes, creating a black hole on your direct path and forcing traffic onto alternative, less desirable routes.

Presented by: **Dewole Ajao**
At: **The ngNOG Conference 2025**
On: October 16, 2025



BEWARE o!

I am not an RPKI expert so….

I don’t know much of what **A.I.** put in these slides.

But I work closely with networks whose traffic ends up going indirectly when they fail to tidy up their RPKI, so I thought I should let you know about that bit.

Key Takeaways

- RPKI is a vital security feature, but misconfigurations can disrupt optimal routing.
- An **"Invalid"** RPKI status is a primary reason for traffic avoiding otherwise healthy direct peering links.
- The most common cause is simply **outdated or incorrect ROAs** that don't match your live BGP announcements.
- **Proactively audit your ROAs** and use monitoring tools to ensure your direct path is always the preferred path.

Direct Peering ✔

Adequate headroom on all ports ✔

but still large amounts of Indirect Traffic ❗

- You have a high-quality, direct peering connection to content provider.
- Your ports show no signs of congestion.
- Yet, a significant portion of your traffic is routed through transit providers.

What is indirect traffic??

Loosely translated, network traffic that flows into your network via an indirect path when you have an interconnection link (PNI, NNI) that could have been used to reach the destination/origin

Meet the Likely Culprit: RPKI Invalidation

RPKI itself is not the culprit though. It seems RPKI is something that has come to stay - and if we don’t get our acts right as Network Engineers, we will simply be causing our organisations expenditure that could easily be avoided while also degrading the user experience.

Note: Sometimes funny things could also be happening on the side of the content provider to make them route traffic differently for a short period but this is not usually expected behaviour.

What is RPKI?

- **Resource Public Key Infrastructure:** A security framework that adds a layer of trust to BGP, the Internet's routing protocol.
- **Its Goal:** To prevent BGP route hijacking and reduce the impact of misconfiguration by ensuring only authorized networks announce specific IP prefixes.
- **How:** It uses cryptographically signed records called **Route Origin Authorizations (ROAs)** to create a verifiable link between an IP address block and the Autonomous System (AS) allowed to originate it.

How RPKI Works (and Fails)

The Three States of RPKI Validation

When the large scale content provider network receives your BGP route announcement, it may perform Route Origin Validation (ROV), resulting in one of three states:

- ✅ **Valid:** The announcement matches the ROA.
- ❌ **Invalid:** The announcement *contradicts* the ROA (wrong AS or prefix length).
- ❔ **Unknown/Not Found:** No ROA exists for the prefix.

The Crucial Point: Some major networks have a policy to **reject or deprioritize RPKI-Invalid routes.** *Even if they don't do it today, it's probably coming soon.*

Your direct path will very likely be ignored because its route announcement is seen as invalid.

Why Are My Routes Invalid?

Common Misconfigurations That Invalidate Your Routes

- **Outdated or Incorrect ROAs:** The most common issue. Network changes (like re-allocating IP space or changing the originating AS) are not being reflected in your ROAs.

- **"Max Length" Mismatches:** You announce a more specific prefix than your ROA allows. (e.g., ROA for `/22` has `maxLength /23`, but you announce a `/24`).

- **IP Leasing & Third-Party Announcements:** You lease IP space to a customer, but forget to create a ROA that authorizes *their* AS to announce it.

- **Aggregate vs. Specifics:** A ROA for an aggregate block exists, but a more specific announcement is made without its own corresponding ROA.

Impact on Traffic Flow

The Ripple Effect: How Invalids Reroute Your Traffic

Inbound Traffic (Nollywood-Video-Provider to You):

1. Nollywood-Video-Provider network sees your direct peering route as **"Invalid"**.
2. It **rejects** this direct path.
3. It selects the next best *valid* (or unknown) path, which is usually via your transit provider.
4. Your traffic takes an expensive, higher-latency detour.

How to Fix It: RPKI Troubleshooting

1. **Audit Your ROAs:**
    - Log into your Regional Internet Registry (RIR) portal (AFRINIC, APNIC, ARIN, LACNIC, RIPE).
    - Meticulously compare your BGP announcements with your created ROAs. Verify the Origin AS and Max Length for every prefix.
2. **Use the Tools provided by the Content network:**
    - A popular one provides an **ISP Portal** with a **Monitoring** section that provides **"BGP View"**.
    - This shows you *exactly* how their network sees your RPKI status, removing any guesswork.
3. **Leverage Public Monitors:**
    - Use external tools and public looking glasses.
    - These provide a global perspective on your route's validity from different network vantage points. RouteViews anybody?

Key Takeaways

- RPKI is a vital security feature, but misconfigurations can disrupt optimal routing.
- An **"Invalid"** RPKI status is a primary reason for traffic avoiding otherwise healthy direct peering links.
- The most common cause is simply **outdated or incorrect ROAs** that don't match your live BGP announcements.
- **Proactively audit your ROAs** and use monitoring tools to ensure your direct path is always the preferred path.

THANK YOU!