



# How AWS is helping to secure internet routing

**FCC Public Workshop July 2023**

Fredrik Korsbäck

Senior Infrastructure Business Developer

“BGP Guy”

# AWS Global Infrastructure

AWS REGIONS, EDGE LOCATIONS, AND THE GLOBAL BACKBONE



## AWS NETWORK BACKBONE

- 400+ Edge Locations
- 245+ Countries & Territories
- Hundreds of thousands of BGP sessions



# Our Current **toolbox**

- Max-prefix filters on all BGP-sessions globally, based upon PeeringDB data
- RPKI ROAs on **everything**. We **force** BYOIP customers to create and keep ROAs updated.
- RPKI OV on **all** external BGP sessions
- “BGP-Weather”: BGP-table monitoring from a large set of available sources, RIPE RIS live, Qrator, BGPmon, our own BMP data post/pre policy etc.
- Automatic counter-hijack system, if we detect an illegitimate announcer we will match that announcement and globally announce to **snap** traffic back to us.
- Global network of our own sensors trying to “hijack” us in various ways to determine posture of ISPs
- **Delegated** RPKI in US and EU, more to follow. (We think we are more or less alone on this venture among large Internet companies)
- Peerlock in place with able ISPs, continues to lean on as many as possible to enable this feature
- “IRR Counterintelligence”
- Pushing ISP’s hard for years to improve posture. This is a **team effort**.

- More context: <https://aws.amazon.com/blogs/networking-and-content-delivery/how-aws-is-helping-to-secure-internet-routing/>





# Future problems and opportunities **with** solutions

- **ASPA:** The next key-technology for the Internet to get a fair chance on deploying *path validation*. Most likely 3 years out before any meaningful implementation. We are already working with internal and external vendors to be fully ready day1. We are suggesting customers, suppliers and vendors to do the same, prepare **now**
- **BGPSEC:** Perhaps (?) the most sensible bet for long-term cryptographic upgrades to the whole BGP ecosystem. Most likely 7-10 years out. Work starts **now** in closed user groups on feasibility studies. Not slated for internet-wide deployment, but Makes sense for “VIP” BGP-sessions (Very Important Peer...).

# Future problems and opportunities **without** solutions

- **IRR:** Crowd-sourced yellow-pages of Internet infrastructure. The more we look, the more brittle and broken the system is. Tons of broken and unmaintained sources (Basically all except 5). Data-cleanup is needed, we (The Internet) need to take hard decisions on deprecating poorly maintained sources
- **ISPs:** Lack of lowest bar in the Industry. Certain ISPs has no routing security posture at all. Who these are, is known not only by us but also by threat actors and becomes their ISP of choice. There is really large international ISPs in this group that can cause cross-continental outages. MANRS could function as a minimum baseline here?