Dropping RPKI invalid routes in a service provider network

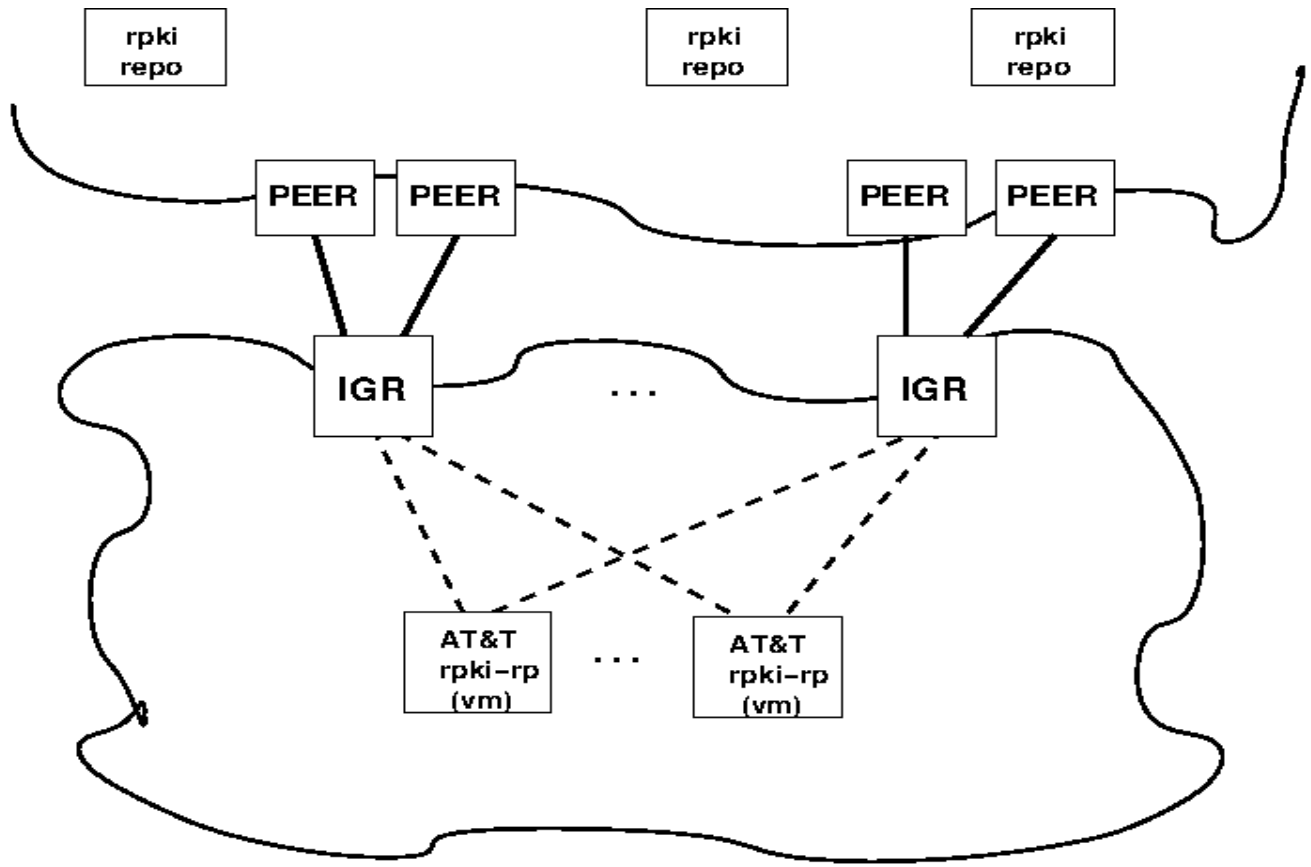
Why RPKI

- RPKI Route Origin Validation is designed to address certain types of route mis-originations (Pakistan Telecom / YouTube 2007)

- Does not fix everything, but we believe it helps enough to be worthwhile

Limitations of RPKI have been discussed extensively elsewhere

RPKI at AT&T


rpki
repo
rpki
repo
rpki
repo
PEER
PEER
PEER
PEER
IGR
...
IGR
AT&T
rpki-rp
(vm)
...
AT&T
rpki-rp
(vm)

Steps leading up to “drop” policy

- Deploy RP caches and establish rtr to routers
- Verify routers are receiving consistent VRPs
- Create policy to tag routes with BGP communities
  - Contact peers to inform them that their customers are originating invalid prefixes
- Use standard netflow tools to analyze traffic flow
  - Need to watch out for covering aggregates
  - Recent tools might make things easier: https://mailman.nanog.org/pipermail/nanog/2019-February/099522.html
- Depreff invalids: much less impact than expected, but useful to see. NOT a long term solution
- DROP

What happened after implementation?

- Mostly nothing ☺
- With roughly 63839 ipv4 / 11252 ipv6 published VRPs learned on our routers, we were made aware of less than 10 reports of lost connectivity.
  - In every case, the owners of the impacted prefixes took corrective action and updated their ROAs to resolve the issue.

Observations

- It seems like many invalid prefixes are due to mistakes
  - Without feedback from networks dropping invalid prefixes, ROAs and real advertisements may have fallen out of sync for some networks.
  - Some operators may have misunderstood the purpose of the ROA and authorized their upstream provider's ASN.
  - Some operators may have published ROAs for their aggregates but not considered that they delegate prefixes to downstream customers.
- Impact so far appears to have been minimal (one week as of the time of this writing). We encourage other networks to deploy.


LET'S
DO
THIS!!
quickmeme.com