Making BGPsec Deployable

What, Why, and When?

Perceptions of BGPsec

- Does it exist at all?
- Won’t work.
- Too slow.
- Need to replace all the hardware.
- Isn’t origin validation enough?
- Not scalable.
- Leaks private information.
- Does not address the real problem.
- Key management is complex.
- BGP is secure anyway.

Horror story

- **Imagine this**

- Your country is at war with another country and your country has a news website , news.com, in a ASn, which the aggressive country do not like.
- The hosting ISP, has created RPKI ROAs to protect the website. **GOOD JOB HOSTING ISP**
- The attacking country creates forged IRR-records in for example AltDB or RADB to “trick” regular IRR-filters. The secret hackertrick to actually be able to do this is to have access to one (1) email-address of any sort.
- The attacker waits 3-4 days for IRR-changes to propagate into larger carriers through standard operations of the IRR-tools used.
- The attacker has access to one or many well-connected large networks that now updated their IRR-filters to include news.com IP-space.
- The attacker send in the routes with forged origin (but RPKI Compliant) and RTBH-communities to cheat both IRR and RPKI filters.
- Now this website is blackholed in large parts of the world.
- There is no technology the hosting-party or upstreams could have implemented to stop this in 2022.

- Ergo: RPKI, ASPA and IRR does not seem to be enough, we need to look for origin protection.

BGPsec basics

- Cryptographic validation of traversed AS path
- For external BGP only
- Transit nodes sign the current AS path and forward AS hop too.
- Each individual prefix is signed separately.
- Regular DSA scheme based on asymmetric cryptosystem.
- Signing, not encryption.
- Operation relies on presence of RPKI data.

Another horror story

When Tier-1s are deceived...

- A few months ago a large cloud provider was brutally assaulted
- There is a domain pattern “asXXX.net” (example: as2914.net)
- Created domain, created a few RADB objects, ordered ports from Tier-1 providers pretending to be noc@asXXX.net
- Then the BGP hijacks started: really nasty to troubleshoot! Correct origin, correct adjacencies, very painful.

Customer views - IXP

- BGPsec mandates end to end operation.
  - Which is unrealistic to expect on a global scale.
- IXP might be a good starting point.
  - IXPs keep traffic – and routing – local. Basically, IXPs are islands of routing
    - Perfect for incremental deployment of BGPsec
  - IXPs routing is hidden to BGP public route collectors
    - It is hard to detect hijacks and react, unless local mechanisms are applied
  - AS paths in IXPs are very short
    - Cryptographic operations would be minimal = no hardware update/change required?
- Gains (security) may outweigh costs in IXP case

Regulator views

- Nothing specific to BGP in the Finnish regulation
  - IP address spoofing is prohibited (BCP38 and BCP84 mentioned in regulation 67 of Traficom)
- Roughly 37% of routes seem to have RPKI
- ~26% of AS use RPKI
- We can regulate you more if it’s helpful :)

Vendor views

- BGPsec at this time is materialized (mostly) in opensource
- Commercial vendor implementations are behind
- Both are needed for practical deployments
- Implementations are driven by user base requirements.

Plans and timelines

- Let’s be realistic – global end to end BGPsec deployment is not too likely.
- Limited domain deployments are very likely.
- A few years to get implementations streamlined and gather initial operational experience.
- Second half of this decade for deployments of BGPsec becoming a best common practice.

Open discussion

https://www.bgpsec.net