# draft-ietf-grow-bgpopsecupd-01

Where we are and where we (should) go.

Tobias Fiebig[1]

[1]Max-Planck Institut für Informatik

Nick Hilliard[2*]

[2]INEX

# Changes since -00 (1/2)

- Clarified scope (excl. DC BGP)
- Addressed comments on TCP-AO
- Addressed comments on VRF confinement/OOB/IB for Controlplane Protection
- Contextualized iBGP TCP Auth
- Added note on using a VRF for IXP peerings
- Expanded on AS_PATH filtering/manipulation
- Added extended communities to scrubbing, added in/out scrubbing
- Expand attribute scrubbing, add attribute healing

# Changes since -00 (2/2)

- Included note on not using communities to signal validation state
- Clarified connection between ASPA and OTC
- Added note on filter Idempotency
- Added section on behavior at IXPs, incl. not using LOCAL_PREF and honoring GSHUT
- Explicitly reference issues with MED induced route oscilation
- Shortened abstract
- Fixed a logic-error in the reference to aspa
- Set the document to obsolete RFC7545, if approved
- Nits (Term alignment, fixing references)

# All Eggs in One Basket

- Currently, the draft tries to be *comprehensive* and include ‘everything that is known now’
- Makes it difficult to reach eventual rough consensus; The document will (potentially) take years
  - People will always find *THAT ONE SHED!* to be specific about
  - Reality will change faster than the document ever could
  - Unclear when something is stable enough to be included
- Terms list is *also* in there (like RFC8499 (DNS Terminology), but just a subsection)
- In general, neither BCP194, nor the current I-D, are abstract enough to be “timeless” (several points noted in read-through actually verbatim from 194)

# Global Policy Developments

- Policymakers are looking for ‘guidelines’ on what they can require in terms of ‘cyber’-security for “Critical Infrastructure”
- Policymakers tend to be ‘a little less familiar’ with the nuances between ‘should’, ‘SHOULD’, ‘must’, and ‘MUST’ than would be required to understand the nuances of the document (“My network, my rules.”)
- Policymakers like things that are ‘testable’, i.e., can be ‘certified’.
- Policymakers *did* find BCP194, and *do* reference it in policies
- While one may be able to ignore no longer sensible parts of a BCP, this is difficult with laws.

# BCP194 Compliance: Priors

- BCP194 recommends announcing IXP-LANs with the RS, or each peer to their cone with their own ASN
  - RIPE-804 sets the minimum v4 size for IXP allocations to /26 (ARIN_prop_320 is similar)
  - Some IXPs use a /64 v6 for different peering LANs
- IXPs and ISPs tend to be critical infrastructure
- Terminology (peer, peering, peering session) is ambivalent in BCP194

# BCP194 Compliance: A Worst-Case

Expressing an absolut (yet not impossible) worst-case law in BCP194 terms:

- IXPs MUST announce their peering LAN prefixes if they are considered critical infrastructure.
  - → Up to /64 v6 and up to /26 v4 MUST be accepted from all BGP neighbors
- ISPs MUST announce the peering LAN prefixes of all IXPs thei are connected to, if these do not announce them.
  - → IXPs MUST create route-objects for all members for the peering LAN
  - → ISPs MUST announce prefixes they are not authorized to aanounce
- ISPs and IXPs MUST use IRRtool to generate prefix filters
- ...

→ 'Not an ideal outcome of the policy making process.'

# Options forward: Beyond BCP194

- Split out individual eggs from the current draft:
  - Keep the core of the document that focuses on timeless truth about BGP security (purpose/goals/high-level), which can replace BCP194 as a BCP
  - An informational document listing ‘the basket of eggs’ that is there in terms of what can be done to secure BGP
  - An informational document reporting terminology ‘as used in drafts around the time of writing’
- Be. Quick; Before things become laws.

# draft-ietf-grow-bgpopsecupd

Focus should be on:

- Short enough for policymakers to read
- Generic enough to be resilient to specific technology changing
- Testable independent of implementation
- Published quick enough to prevent harm (more months than years)

# Securing BGP: A list of techniques

- Lists *possible* ways of accomplishing what the policy document should require.
- Different techniques can be neutrally described w.r.t. the issue they solve and what caveats exist without making value statements on whether they should (not) be used; See also the MTA-STS vs. DANE discussion.
- Enables a more extensive list that can be more easily updated than a BCP, without risking consensus-potential by having too many knobs.

# Terminology Document

- A document similar to RFC8499/BCP219 (DNS Terminology), but for BGP (related) terms
- Descriptive instead of BCP given changing nature of routing and a need to have easier consensus
- Basically like the ‘techniques’ document, but for terms; Regularly updated, documenting terms and how they are used (Oxford vs. French style)

# Discussion Startingpoints

- BCP194 must change quickly
  - Claim: We have consensus *that* it needs changing, question is how
  - If we wait too long, we may no longer be able to change it.
  - Focusing on a draft that creates a high-level/vision policy will enable quicker consensus by avoiding bikeshedding around technology.
  - A policy driven draft will also be more robust against technology changing

  → Plan would be for Nick & me to update and slim the document for the list the week after 119

- Moving terminology and 'implementation options' to informational documents makes consensus easier, as they do not codify

  → We have time for these and can draw heavily from text to be cut from draft-ietf-grow-bgpopsecupd-01.