draft-ietf-grow-bgpopsecupd-03

Keeping it short(er).

Tobias Fiebig[1]
[1]Max-Planck Institut für Informatik

Nick Hilliard[2]
[2]INEX

The plan from IETF119

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)

Split out individual eggs from the current draft basket:

- ✓ 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.**

The plan from IETF119

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)

Split out individual eggs from the current draft basket:

✓ 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.**

The plan from IETF119

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)

Split out individual eggs from the current draft basket:

✓ 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.**

Changes since -01

- Removed text that is not ‘time-less high level directive policy’ since -00
  - Has been ‘reserved for future use’ in draft-fiebig-grow-routing-ops-sec-inform and draft-fiebig-grow-routing-ops-terms (later more)
- Removed some more; Around 90% of it.
- Focused on the essentials:
  - Do not expose your BGP speaker unnecessarily
  - Make sure you do not import NLRI from people not authorized to advertise them to you
  - Make sure you do not export NLRI to people you are not authorized to advertise

3.1. BGP Session Protection

- Prevent off-path attackers from injecting BGP messages into existing sessions.
- Prevent off-path attackers from interrupting existing sessions.
- Prevent off-path attackers from preventing the establishment of new sessions.
- Prevent remote systems from overwhelming the BGP speaker by sending large volumes of unsolicited packets or BGP messages.
- Ensure that unstable sessions do not threaten the availability of BGP speakers within the network.

3.2. BGP Speaker Mgmt. Interface Protection

- No unauthorized third-parties can obtain access or connect to the management interface of a BGP speaker in a way that allows tainting confidentiality, integrity, or availability.
- External activity towards the management interface do not interfere with the integrity or availability of BGP sessions.

4.1. Importing NLRI

- The AS originating NLRI for a prefix MUST be globally authorized to originate that prefix. Operators MAY deviate from this for default routes (::/0 and 0.0.0.0/0), if they granted the specific neighbor permission to announce default routes towards them.
- The AS_PATH of the NLRI MUST NOT violate the valley-free principle [RFC4012], i.e., all ASes left of the originating AS in the AS_PATH MUST be authorized to advertise the NLRI to the AS directly to their left.
- The AS_PATH MUST NOT contain AS numbers reserved for private [RFC6996] or special-use cases not necessitating their presence in the global routing table [IANAASNSpec].
- The number of NLRI received from a neighbor MUST NOT exceed the resources of the local router.

4.2. Originating and Redistributing NLRI

- The AS_PATH of redistributed NLRI MUST NOT violate the valley-free principle [RFC4012], i.e., the redistributing AS MUST be authorized to redistribute NLRI for the specific prefix when received from the AS directly to its right in the AS_PATH. Additionally, each AS in the AS_PATH not originating the prefix MUST be authorized to redistribute the prefix when receiving it from the next AS to its right.
- The AS originating NLRI for a prefix MUST be globally authorized to originate that prefix. Operators MAY deviate from this for default routes (::/0 and 0.0.0.0/0), if they originate the default route and the specific neighbor granted them permission to announce default routes towards them.
- The AS_PATH MUST NOT contain AS numbers reserved for private [RFC6996] or special-use cases not necessitating their presence in the global routing table [IANAASNSpec].

4.3. General Considerations for Altering NLRI

- An operator MUST NOT change transitive BGP attributes, if the attribute is unknown to the operator. In selected cases, if a specific attribute is known to be malicious, an operator MAY filter that specific attribute or the NLRI.
- NLRI carried on BGP MUST NOT be enriched with transitive attributes subject to change independent of the underlying NLRI, e.g., encoding RPKI validation state in transitive attributes [I-D.spaghetti-sidrops-avoid-rpki-state-in-bgp].

Next steps

Reach WG consensus on:

- What can still be taken away?
  - ⇒ There is not much left
- What should be added?
  - ⇒ Suggested metric: If there is more than two mails/minutes of discussion on **if** it should be added, it belongs in draft-fiebig-grow-routing-ops-sec-inform.

When we are there ⇒ WGLC?

Discussion Starters

- From 119: 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
- We got a *very* slim draft now; How do we move forward *quickly*?