BGPSEC Protocol
Resolving Last Call Comments

Matt Lepinski – BBN Technologies

Working Group Last Call

- Working Group Last Call : Jan 26 – Feb 9
- Thanks to everyone who sent comments!
- Goal: Next version of document to IESG

Issue 1: Deferred Validation Visibility

- Suggestion:
  Clearly recommend that if deferred validation happens, the implementation should make this visible to the operator. (E.g., log messages, bgp diagnostic information.)

- Proposed Resolution:

  Yes, include this recommendation

Issue 2: Policy Regarding Validation State

- Suggestion:
  Clearly indicate that local policy regarding use of validation may depend on the ASN from which a route was received. (Note: this is guidance to implementers)

- Proposed Resolution:

  Yes, include this recommendation

Issue 2: Policy Regarding Validation State

- Suggestion:
  Clearly indicate that local policy regarding use of validation may depend on the ASN from which a route was received. (Note: this is guidance to implementers)

- Proposed Resolution:

  Yes, include this recommendation

Issue 3: Possible Signature Attack?

- Possible Attack:

A valid origination signature is re-used a valid signature on a

- Proposed Resolution:

Attack cannot happen as it would require that a signature could be parsed {Alg. ID, NLRI length, NLRI prefix}. That would require a 6-octet or 18-octet (IPv6) signature. Signatures cannot possibly be that short.

Insert security considerations text

Issue 4: Signing the AFI

- Issue:

Given that the AFI is unsigned, there appears to be ambiguity between signing 1.2.0.0/16 (IPv4) and 1020::/16 (IPv6)

- Proposed Resolution:

Add AFI to the structure that is signed by the originating AS

Issue 5: NLRI Trailing Bits

- Issue:

RFC 4271 (and RFC 4760) both say that for BGP, the trailing bits between the prefix and the octet boundary are irrelevant.

What if two implementations set these bits in different way?

- Proposed Resolution:

Make explicit that implementations MUST treat these trailing bits as zero for the purpose of signature calculation/verification

Issue #6: AS Migration

- Issue:

In I-D.sidr-as-migration (Section 5.2), a router configured to do AS migration shall:

1. Generate a signature for the old (local) ASN signing towards the new (global) ASN
2. Attach the signature to the update sent to iBGP peers

In BGPsec, one does not typically attach new signatures when sending to iBGP peers.

Proposed Solution:
I-D.sidr-as-migration is correct. Clarify this is in BGPsec protocol.

Issue #7: Multiprotocol Extensions

- Issue:

If a BGPsec speaker does BGPsec only for IPv4, must the BGPsec speaker advertise support for RFC 4760 (multiprotocol extensions)?

If Yes, is the IPv4 NLRI sent in the MP_REACH_NLRI attribute?

- Proposed Resolution:

???

Moving Forward

- I believe this captures all WGLC comments on the list that would change the behavior of an implementation
- If you sent something to the list and it is not here, then somehow I missed it. Please let me know ASAP
- Next version of the draft will include resolutions for these issues and should be ready to send to the IESG