NIST National Institute of Standards and Technology

iTL INFORMATION TECHNOLOGY LABORATORY

# Decoupling BGPsec Documents and Extended Messages draft

**K. Sriram**

Acknowledgements: Thanks to Alvaro Retana and Sue Hares for comments and suggestions on the slides.

**IETF SIDROPS Working Group Meeting, IETF-98**
**March 2017**

# Extended messages draft status

- Back with the IDR WG
- It may take a while to settle

# BGPsec spec

- BGPsec spec currently says:
  - ➢ SHOULD negotiate extended message before negotiating BGPsec capability

# BGP and BGPsec Update Sizes

| | Update size (bytes) | |
|---|---|---|
| | BGP (including Attributes, Community) | BGPsec (Prefix and BGPsec_PATH) |
| Average | 68 | 422 |
| Maximum | 333 | 1542 |
| | Note: Measured from Routeviews data (March 2017) | Note: Estmated based on [Huston] data |

- ECDSA P-256 signature size is 64 bytes.
- Extended message was thought to be necessary when RSA-2048 (256 bytes sig) was initially proposed.
- In the Internet, the observed average and maximum AS path lengths are 3.8 and 15, respectively [Huston]. These have remained in this ball park for many years now.

[Huston] G. Huston, "AS6447 BGP Routing Table Analysis Report," March 13, 2017. http://bgp.potaroo.net/as6447/

# What is Proposed?

- Alvaro's suggestion (speaking as WG member):
  - Just mention the "maximum message size" (with no specific numbers).
  - This way the BGPSec documents:
    1. Don't depend on the Extended Messages document, and
    2. They depend on whatever BGP can do. If/when Extended Messages are settled and implemented, then BGPSec can make use of them (as can any other application using BGP).

# Proposed Rewording

- Delete from BGPsec draft:

  "…any BGPsec speaker announcing the capability to receive BGPsec messages SHOULD also announce support for the capability to receive BGP extended messages…"

- Add the following new wording in Section 4.2:

  **BGPsec update size is subject to a maximum BGP update size.**

- Further, …. see next page

# Proposed Rewording

- If the sending router determines (albeit highly unlikely) that adding its Secure_Path Segment and Signature Segment causes the BGPsec update to exceed the maximum size, then the router ……..
  - Need WG input on this
  - Possible choices:
    - converts the BGPsec update to an unsigned traditional BGP update and sends the unsigned update.
    - does not send the update.
    - ??

Note: BGPsec spec already allows conversion to unsigned update when sending to a non-BGPsec neighbor.