Draft-ietf-sidr-bgpsec-protocol

Matt Lepinski

Minor Issue: multiple BGPsec attributes

- Thanks to Michael Baer for catching this issue
- Next version will clearly indicate that multiple BGPSEC_Path attributes are treated as a withdrawal

Open Issue: AS Migration

- Draft-ietf-sidr-as-migration describes how to use BGPsec in an AS number migration scenario
- My plan is to reference as-migration in bgpsec-protocol.
- However, if the working group prefers, I could incorporate text from the as-migration draft directly into the protocol document.

Open Issue: Origin Validation

- Sandy Murphy suggested on the list that BGPsec should reference the origin validation algorithm in RFC 6811/6483.
- We could probably do this in such a way that BGPsec inherits any changes we might make to the origin validation algorithm
- We should either do this, or else completely remove origin check from BGPsec validation algorithm

Requirements Analysis

- Draft-ietf-sidr-bgpsec-reqs has been approved by the IESG
- I believe that almost all of the requirements are met by the current protocol version
- This presentation contains only those requirements that might require additional discussion.

Requirement 3.5

“3.5   A BGPsec design MUST provide analysis of the operational considerations for deployment and particularly of incremental deployment, e.g, contiguous islands, non-contiguous islands, universal deployment, etc.”

Requirement 3.5

- Please read draft-ietf-sidr-bgpsec-ops
- If you think the text in bgpsec-ops is insufficient, please send concrete suggestions for improving the ops document.

Requirement 3.8

“A BGPsec design MUST resist attacks by an enemy who has access to the inter-router link layer, per Section 3.1.1.2 of [RFC4593]. In particular, such a design MUST provide mechanisms for authentication of all data, including protection against message insertion, deletion, modification, or replay. Mechanisms that suffice include TCP sessions authenticated with TCP-AO [RFC5925], IPsec [RFC4301], or TLS [RFC5246].”

Requirement 3.8

- Currently, BGPsec protocol says SHOULD use transport or network layer mechanisms to secure the link between routers.
- Should BGPsec protocol include either a MUST implement or a MUST use mechanism?
- Or perhaps a mandate: MUST use one of several “acceptable” mechanisms?

Requirement 4.3

“Replay of BGP UPDATE messages need not be completely prevented, but a BGPsec design SHOULD provide a mechanism to control the window of exposure to replay attacks.”

Requirement 4.3

- The working group consensus was that RPKI mechanisms were sufficient to limit the window of exposure to such attacks. (At least for the initial release of BGPsec)
- There is currently text in Section 8 of the ops document.
- Proposal: Add a sentence to the security considerations on this issue with a reference to the ops document