BGPSEC router key rollover as an alternative to beaconing

draft-ietf-sidr-bgpsec-rollover-01

Roque Gagliano

Keyur Patel

Brian Weis

Summary of draft

- Describes a method for rolling over BGPSEC router keypairs/certificates
  - Since the replacement of a router keypair has the effect of invalidating BGP UPDATE messages signed with the old key, an orderly rollover is required
- We note that a BGPSEC key rollover can be used as a measure against replays attacks in BGPSEC

Changes in -01

- Addressed comments received from Steve Kent and Kotikalapudi Sriram
  - – Thanks much!
- We believe a new revision of the draft will be required once the WG advances on key provisioning and the RTR protocol.

Questions for the WG

1. Change of I-D name: The individual I-D name was a provocation to start debate on alternatives to beaconing. ☺
2. Standards-Track or BCP?
   - Currently targeting Standards-Track.
   - However, the RPKI rollover document is BCP and contains no normative text in the document, even if replay attack protection is a BGPSEC requirement.
   - Our preference is for BCP.