Draft-ietf-sidr-bgpsec-protocol-00

Matt Lepinski (editor)

BBN Technologies

What is BGPSEC?

- Mechanism for securing the AS-PATH attribute

- Extension to BGP that is negotiated as a new capability (RFC 5492)

- An optional path attribute that contains a list of cryptographic signatures that protect the AS-PATH

- See IETF 80 presentation at:
  - http://www.ietf.org/proceedings/80/slides/sidr-18.pdf

Draft-ietf-sidr-bgpsec-protocol-00

- BGPSEC was adopted a working group document to meet the chartered milestone for AS-PATH security

- The working group document has no normative changes from draft-lepinski-bgpsec-protocol-00
  - Changes are all clarifications to text based on feedback from Prague

- This is still a -00 document very much a work in progress!

Related Documents

- Draft-ietf-sidr-bgpsec-overview:
  - High-level overview of the bgpsec related documents
- Draft-ietf-sidr-bgpsec-threats:
  - Threat model for BGP Path Security
- Draft-ietf-sidr-bgpsec-reqs:
  - Requirements for BGP Path Security
- Draft-ietf-sidr-bgpsec-ops:
  - Operational considerations for BGPSEC deployments
- Draft-sriram-bgpsec-design-choices:
  - Historic documentation of how we got to -00

(Very) New Related Documents

- Draft-turner-sidr-bgpsec-pki-profiles:
  - Extends the RPKI to include certificates with BGPSEC keys
- Draft-turner-bgpsec-algs:
  - Defines cryptographic algorithm suites for BGPSEC

Mailing List Discussion

- Thank you to everyone who has participated in mailing list discussions related to BGPSEC
  - Special thanks to those who read the document and provided reviews/feedback!!

- Two broad topics will be addressed at this meeting:
  - Beaconing / Replay protection / Expire Time
  - Route Servers / AS Prepending / Transparency

- Due to time considerations, we welcome discussion of other topics on the mailing list