Update on BGPsec Reference Implementation BGP-SRx

&

BGPSEC-IO

More than just a BGPsec Traffic Generator

IETF 99

Prague, Czech Republic
July 17, 2017

Oliver Borchert (oliver.borchert@nist.gov)
National Institute of Standards and Technology

Update since IETF 97

- Added support for RFC-to-be 8210
  - Allow sending and receiving router keys
- Moved BGPsec path validation from QuaggaSRx to SRx-Server
- Modified code to IANA assigned values
    - BGPsec Capability 7 (previously used 72)
    - BGPsec_PATH 33 (previously used 30)
  - Added compiler parameters allowing to use previously used values for backwards compatibility (e.g. BIRD)

SRx Improvements in ROA processing

- Previous implementation:
  - Each individual ROA change triggered the decision process to run
    - This caused unnecessary churn depending on the order in which ROAs were received and processed
- Newest implementation:
  - The decision process gets triggered once the RPKI cache update is finished (after END OF DATA)

BGPSEC-IO - Intention

- What we needed…
  - … a **traffic generator** for multi hop fully signed BGPsec updates (RFC-to-be 8205)
  - … a tool for **performance measurements** of BGPsec path validation
- What we wanted…
  - … a tool for **printing** BGPsec update traffic in human readable form
  - … a tool for **generating** BGPsec **test vectors**

BGPSEC-IO: Traffic Generator

- Generation of multi hop fully signed BGPsec update messages
  - Originator, Intermediate, eBGP, iBGP
- Storing of generated BGPsec update into binary file
  - Fast replay without signing delay
- Easy to script updates
    - Format: <prefix>[,[<asn[p<count>]>]+]?
    - Example: 10.0.0.0/8
      10.0.0.0/8, 65535
      10.0.0.0/8, 65535 65535
      10.0.0.0.8, 65535p2 65536
  - Can be scripted in configuration, as parameter, or piped file
  - Update order: session, global, command line, binary file

– Hold BGP session until last update was send, for x minutes after last update was send, or until peer closes session .

BGPSEC-IO: Crypto Tester

- Generation of multi hop fully signed BGPsec_PATH attribute
- Measurement of validation time only
  - Generation of the BGPsec_PATH attribute and loading of necessary keys is not included in measurement .
- Generates a final statistic for both validation results: valid and invalid

BGPSEC-IO:
Internal BGPsec Crypto Engine

- Signing engine independently implemented from BGP-SRx
- Generate fully signed BGPsec path (RFC-to-be 8205)
  - Normal operation (regular ECDSA p-256 operation)
  - Using preselected ‘k’ − RFC 6979 to generate deterministic signatures
    - Two ‘k’ values to choose from
    - Allows debugging of peer crypto engines or SRxCryptoAPI
- Fallback method for failed signatures due to invalid or missing private key
  - DROP (skip update generation),
  - Generate BGP4 AS_PATH (no crypto),
  - FAKE pre-scripted signature & SKI (configuration file).
  - Can be replayed for crypto tester (incl. traffic generator)

BGPSEC-IO: Player

- Pre-generated BGPsec / BGP UPDATE traffic:
  - Binary file contains BGPsec updates as well as regular BGP updates depending on fallback settings
  - Public keys must be pre-distributed to routers
  - Deterministic traffic (due to replay)
  - No delay due to signing
- Pre-generated BGPsec_PATH attributes for testing the SRxCryptoAPI do provide also the public keys needed for path validation.
  - No need to pre-distribute public keys to SRxCryptoAPI, key registration is performed prior validation call

BGPSEC-IO: Printer

- Print BGP and BGPsec update messages in human readable form
  - Followed Wireshark format
- Configure BGP update types to be printed
  - None, All, or selective:
    UPDATE, OPEN, NOTIFICATION, and KEEPALIVE
  - On send, on receive, or both
- Allows BGPSEC-IO to be solely used as traffic receiving printer

BGP-SRx and BGPSEC-IO

- BGPSEC-IO is part of the BGP-SRx software suite and is open source.
- The software can be downloaded from:

https://bgpsrx.antd.nist.gov

- Send questions to: oliver.borchert@nist.gov