BGP Transport Security

Do you care?

Context

- BGP transport security (MD5).
- Not BGP information security (BGPsec, RPKI family).

- MD5 is considered to be unsuitable for its purpose.

- Security community is unhappy with MD5 usage.
- Security community does not always have full insight on how MD5 is used in routing environments.

BGP Security

- BGP relies on commodity underlying transport for its operation.
- BGP itself does not have its own key management, and confidentiality or integrity validation mechanisms.
- BGP information security makes assumptions on presence of BGP transport security.
- Does that mean that BGP security is inherently broken?

Majority of security issues with BGP lie on the BGP information security side. Transport security is perceived to be not that important.

BGP and Transport

- TCP (today).
- Attacks on TCP are rather trivial.

- TCP Authentication.
- Has been around for long.
- Validates transport session authenticity.
- No stray rejects.
- No tampering of payload.
- No confidentiality (= no encryption of payload).

TCP Authentication Mechanisms

- TCP-MD5. Universally supported, works, has operational limitations. Has perception of being broken.
- Enhanced TCP-MD5. Limited to a group of vendors. Addresses many of the limitations of TCP-MD5. Generally not interoperable.
- TCP-AO. Solves most of the problems. It does not exist in practice.
- A few niche vendor proprietary mechanisms.

Best Practices

- Apply proper TTL settings and use GTSM.
- Use proper edge filtering.
- Use graceful restart.
- Proper network design.
- Proper operational hygiene.

- Use session authentication.

Requirements for Transport Security

- Long lived sessions.
- Algorithm agility.
- Initial key synchronization.
- Key rollover.

- Must be practically usable by operators.
- Must be practically implementable by vendors.

Transport Options

- TLS does not authenticate TCP header.
- Certificates used for TLS have validity time.
- IPsec (transport mode).
- BGP over QUIC.
- MACsec.
- We can always define a new transport protocol for BGP. :-)
- TCP-AO (in theory).

Do you care?

- Is this a problem worth solving?

- Can this result in a practical solution?

Discussion

- Initial key synchronization?
- Long lived sessions?
- Key rotation?
- Algorithm selection?
- TCP-AO?
- BGP over alternative transports?