BGP Transport Security

Do you care?

The 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 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.
- Confidentiality vs authentication.
- Graceful Restart.
- Proper operational hygiene.

There is little point of having armoured front door when you have no back wall.

TCP Authentication Mechanisms

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

BGP session authentication is more of an operational mismatch detection.

TCP Authentication Mechanisms

- None. It just works.
- 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.
- TCP-AO. Solves most of the problems. It does not exist in practice.
- A few niche vendor proprietary mechanisms.

Best Practices

- Apply proper TTL setting and GTSM.
- Use proper edge filtering.
- Use Graceful Restart.
- Proper network design is key.
- Even with proper network design you need to rely on proper operational hygiene.
- Protocol level security is not a substitute for proper network design.

Requirements for Transport Security

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

Transport Evolution

- TLS does not authenticate TCP header.
- Certificates used for TLS have validity time.
- IPsec transport mode may be an option. It adds noticeable complexity.
- We can always define a new transport protocol for BGP. :-)
- BGP over QUIC.
- MACsec.

BGP will happily rely on whichever transport security option gets chosen.

Summary

- Proper operational hygiene is a must (GTSM, filtering, GR).
- Security mechanisms are not a substitute for operational hygiene.
- Security mechanisms are not a substitute for proper network design.
- Protocol level security mechanisms are an integral part of overall security solution.
- TCP-AO is a good option – please voice your support. We as an industry have a sad situation around TCP-AO.
- In a longer term BGP might run over QUIC.

Do you care?

Is this a problem worth solving?

Discussion

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