TCP Authentication

draft-bonica-tcpm-tcp-ao-algs

draft-bonica-tcpm-extended-options

Background

- Threat: TCP blind reset attacks
  - Attacks against BGP have destabilized networks
- Mitigation: TCP-AO
  - Appears in every segment, including the SYN
  - Currently supports HMAC-SHA-1-96 and AES-128-CMAC-96
    - No longer sufficient
- Draft-bonica-tcpm-tcp-ao-algs
  - SHA-2 and SHA-3 truncated to 128-bits
  - SHA-2 and SHA-3 untruncated
    - Long MACs produce long TCP-A0 68 bytes

Challenges

- Truncated SHA-2 and SHA-3 present no challenges
- Untruncated SHA-2 and SHA-3 challenge TCP's 40-byte option limit

Potential Solutions

- Draft-ietf-tcpm-tcp-edo
  - Adopted by WG in 2014
  - Does not support extended options in SYN
    - Possibly augmented by draft-touch-tcpm-tcp-syn-ext-opt
- Draft-bonica-tcpm-extended-options
  - Individual contribution (EXPERIMENTAL)
  - Supports extended options in the SYN
  - Supported by running code
    - Ready to ship
    - No codepoints required

Active Questions

- How immediate is the requirement for untruncated authentication algorithms in TCP-AO?
- Are strong authentication algorithms required in SYN segments?
  - If so, how immediate is that requirement?
- Are both approaches compatible with legacy TCP implementations?

A Path Forward

- Continued mailing list deliberations
  - Take the time required to make the right decision
- Separate threads (thanks to Lars Eggert):
  - A discussion of requirements
  - A discussion of solutions
- Allow draft-bonica-tcpm-extended-options to proceed as EXPERIMENTAL
  - In case an immediate solution is required

What Is The Risk?

- EXPERIMENTAL status
  - No codepoints required
- If the experiment fails
  - We learn something
  - We end the experiment
- If the experiment succeeds
  - It informs the long-term solution
  - Long-term solution can be backwards compatible with the experiment
  - Long-term solution can obsolete the experiment